

مركز البحوث

أمن شبكات المعلومات

تأليف

حسن طاهر داود

بسم الله الرحمن الرحيم



مركز البحوث

أمن شبكات المعلومات

تأليف

حسن طاهر داود

١٤٢٥هـ - ٢٠٠٤م

بطاقة الفهرسة

ⓒ معهد الإدارة العامة ١٤٢٥هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

داود، حسن طاهر

أمن شبكات المعلومات/حسن طاهر داود-الرياض، ١٤٢٣هـ

٤٢٤ ص، ١٧× ٢٤ سم

ردمك: ٩٩٦٠-١٤-١٠٨-X

١-أمن المعلومات ٢-شبكات المعلومات أ-العنوان

ديوى ٠٠٥,٨ ١٤٢٣/٦٤٥٨

رقم الإيداع:١٤٢٣/٦٤٥٨

ردمك: ٩٩٦٠-١٤-١٠٨-X

إهداء

إلى المهندس/ كريم حسن طاهر داود ..
الشبل الذي آثر أن يسير على الدرب نفسه..
وأرجو الله ألا يلقى العناء نفسه..

حسن طاهر داود

شـــــكـر

أود أن أتوجه بالشكر إلى مدير عام معهد الإدارة العامة معالى الدكتور عبدالرحمن الشقاوي، وإلى مدير عام مركز البحوث بالمعهد سعادة الدكتور صلاح بن معاذ المعيوف، وإلى أعضاء لجنة البحوث بالمعهد لدعمهم وثقتهم التي احتجت إليها كثيرًا لأنهي هذا العمل.

وأتوجه بالشكر إلى عائلتي الصغيرة.. زوجتي الدكتورة/ سهير عبدالحي وأولادي مروة وسارة ومهند وياسر الذين عانوا كما عانيت خلال فترة إعداد هذا الكتاب، ومعهم إخوتي الأعزاء لدعمهم وتشجيعهم.

أود أن أقدم الشكر كذلك للأستاذ محمد توفيق إبراهيم مدير المركز العصري للكمبيوتر بالقاهرة الذي بذل وزملاؤه جهدًا كبيرًا في تصميم إخراج رسوم هذا الكتاب.

محتويات الكتاب


المقدمة

المقدمة:

الحمد للّه .. والصلاة والسلام على رسول اللّه.

المعلومات.. هي سمة العصر الذي نعيشه، حتى أن البعض أطلق عليه عصر المعلومات. وتكتسب المعلومات أهميتها من انتشارها، ومن تبادلها بين البشر. وما كان لهذا العصر أن يكون عصرًا للمعلومات لولا وجود الشبكات، شبكات المعلومات، التي كانت الخلايا العصبية التي تولت نقل المعلومات عبر الدول. وبخروج المعلومات، التي كانت على الدوام مخزنة في أجهزة الحاسبات، بخروجها إلى الشبكات وإلى الفضاء وبانتقالها من قارة إلى أخرى، حملت معها آفاقًا جديدة رائعة للبشرية والإنسانية. وبقدر ما حملت معها من آمال وأحلام وتوقعات واعدة، فإنها حملت معها من المخاوف الأمنية، وخلقت من المخاطر والمشكلات قدرًا مماثلاً.

أصبح هاجس أمن المعلومات خلال رحلتها في الشبكات أمرًا يقلق بال الجميع ممن يتداولون المعلومات.. ومن منا لا يدخل في هذه الزمرة. ثم جاء طوفان الإنترنت.. جاء يحمل معه المزيد من الوعد والمزيد من الوعيد، فأمن المعلومات لم يشهد في تاريخه خطرًا كخطر الإنترنت.. مهاجمون ومقتحمون مغامرون يقضون الساعات الطوال في محاولة اختراق مواقع الآخرين. ثم بدأ هؤلاء يتحولون إلى محترفين احترفوا اختراق المواقع وارتكاب العديد من الجرائم.. ولا يمكن أن نغفل فيروسات الحاسب التي أصبحت لها مواسم تجتاح فيها شبكات العالم وأجهزته، لتخلف الدمار بأشد وأبشع مما تفعله العواصف والأعاصير.

تعددت الأخطار التي تحيط بشبكات أمن المعلومات، ولكن العلم كانت له كلمته، فظهرت أجهزة وتقنيات متقدمة تقاوم كل أساليب انتهاك المعلومات، بل وتجهضها قبل أن تولد. وكان لابد من الإحاطة بكل هذا.. بالخطر القائم من ناحية وبوسيلة المواجهة من ناحية أخرى.. أي بالسم والترياق معًا، ولذلك كان هذا الكتاب.

بدأنا الكتاب في فصله الأول بالحديث عن "الأمن في عصر المعلومات"، حيث أبرزنا

سمات عصر المعلومات كشبكة الإنترنت واستخداماتها الحديثة كالتجارة الإلكترونية والواقع الافتراضي وتطبيقاته، وتحدثنا عن الأخطار المتزايدة التي تحملها التقنية على أمن هذه المعلومات. وأوضحنا في هذا الفصل أثر شبكات المعلومات على أمن هذه المعلومات، والحاجة إلى بيئة معلوماتية آمنة تزدهر فيها مشروعات الحكومة الإلكترونية والبنوك الإلكترونية، وغيرها من المشروعات التي يعتبر أمن المعلومات هو عصب نجاحها.

الفصل الثاني خصصناه للحديث عن أساليب نقل المعلومات عبر الشبكات وأنواع الكابلات الأرضية والبحرية (والفضائية) وعن بروتوكولات نقل البيانات.

ثم الفصل الثالث الذي تناولنا فيه شبكات المعلومات فبينا أهميتها وأنواعها المختلفة، كما تحدثنا عن التقنيات الحديثة المستخدمة في هذه الشبكات، وعن المستقبل الذي ينتظرها، والمشاريع التي تخطط لأحزمة الأقمار الاصطناعية التي سوف تحيط بكرتنا الأرضية.

تناول الفصل الرابع متطلبات الأمن في شبكات المعلومات، فناقشنا فيه المخاطر التي تهددها، وأنواع المهاجمين ودوافعهم. وقدمنا تصورًا جديدًا للنموذج الأمني للمؤسسة، وتحدثنا عن السياسة الأمنية للمؤسسات.

ثم تطرقنا في الفصل الخامس لأساليب انتهاك شبكات المعلومات، ومنها التنصت بأنواعه المختلفة، وإقحام الرسائل في الشبكات، وتزوير المعلومات. وذكرنا كيفية مواجهة ذلك بتقنيات التحقق من سلامة الرسائل. ثم تحدثنا عن أنواع الاقتحام المختلفة، واعتراض البث، وعرقلة الخدمة وأساليبها المختلفة. ثم قدمنا سيناريو لعملية اقتحام ناجحة وخطواتها.

في الفصل السادس كان موعدنا مع الفيروسات، لنكمل بذلك استعراض كل ما يهدد شبكات المعلومات في هذا العصر، فاستعرضنا أنواع الفيروسات المختلفة، ووسائل حماية الشبكات من الفيروسات، وبرامج مكافحة الفيروسات، ثم التوقعات

لمستقبل الفيروسات.

بدأنا في الفصل السابع الحديث عن تقنيات الحماية، فتحدثنا عن التشفير ومتطلبات البنية الأساسية للمفتاح العلني، والتوقيعات الرقمية، وشهادات التعريف الرقمية، وسلطات منح الشهادات الرقمية، والأغلفة الرقمية. ثم انتقلنا للحديث عن الأجهزة والتقنيات الحديثة المستخدمة في مراقبة الشبكات.

ثم تحدثنا في الفصل الثامن عن نظم كشف الاقتحام، فبدأناه بالحديث عن الأساليب الحديثة لاقتحام شبكات المعلومات، ثم عن بعض نظم كشف الاقتحام الحديثة وتقييمها، وعما يتبعه المهاجمون لخداع هذه النظم وكيفية التغلب على ذلك.

خصصنا الفصل التاسع لجدران الحماية، التي تعتبر من أهم وسائل حماية الشبكات. فاستعرضنا أنواع جدران الحماية من مصافي الحزم (الاستاتيكية والديناميكية) وخوادم البروكسي والأجهزة المادية. ثم قارنا بين هذه الأنواع وبينا مزاياها وعيوبها، وتحدثنا عن كيفية تصميم جدران الحماية وتنفيذها، واستعرضنا مجموعة من التقنيات الحديثة المستخدمة في تركيب جدران الحماية.

في الفصل العاشر قدمنا تقنية الشبكات الخاصة الافتراضية، فأوضحنا استخداماتها المختلفة ومزاياها وعيوبها، ثم تحدثنا عن أنواعها وقارنا بينها. ثم تحدثنا عن أسلوب تنفيذ هذه الشبكات واختبار صلاحيتها للعمل.

في الفصل الحادي عشر تحدثنا عن معالجة الكوارث في شبكات المعلومات، وكيفية ملاحقة المجرمين، والإجراءات التي يتعين على المؤسسات اتخاذها لمواجهة اقتحام المهاجمين قبل وقوعه.

في الفصل الثاني عشر والأخير تناولنا تقييم مستوى الأمن في نظم تشغيل الشبكات فقسمنا الفصل إلى ثلاثة أقسام تناولنا في كل منها أحد نظم التشغيل الشهيرة، فقدمنا الأمن في نظام "نتوير" ونظام "ويندوز إن تي" ونظام " يونكس ".

واجهتني خلال إعداد هذا الكتاب مشكلة حقيقية، هي اختيار الترجمة العربية

المناسبة لبعض المصطلحات الفنية، خاصة أن معظم هذه المصطلحات حديث، بل إن بعضها لم يمض عام واحد على ظهوره؛ ولذلك آثرت أن ألحق في نهاية الكتاب مسردين لهذه المصطلحات والترجمة المقابلة لها، أحدهما بالعربية وما يقابلها من الإنجليزية، والآخر بالإنجليزية وما يقابلها من العربية.

كما حرصت على أن أذكر المصطلح الإنجليزي باستمرار مع المقابل العربي في متن الكتاب تسهيلاً على القارئ.

وهكذا حاولنا في هذا الكتاب أن نسهم بجهد ما، قد يساعد على حماية معلوماتنا في عصر قد تكون فيه المعلومات هي الفيصل بين النصر والهزيمة..

وأسأل الله أن يجعل هذا الجهد المتواضع في ميزان حسناتي يوم القيامة.

حسن طاهر داود

الرياض في يناير ٢٠٠٤م

الفصل الأول
الأمن في عصر المعلومات

هذا هو الفصل الأول في كتاب " أمن شبكات المعلومات "، ونعتبره كمقدمة لهذا الكتاب. وكما يبدو من عنوان الفصل، فهو يتناول موضوع الأمن، وكيف اختلف مفهوم الأمن في عصر المعلومات، وكيف اختلفت نوعية المشكلات التي تواجه المسئول عن أمن المعلومات بعد انتشار الشبكات، ودخولنا إلى العالم الرقمي والحياة الرقمية.

نبدأ الفصل بمقدمة عن عصر المعلومات الذي نعيشه وعن أبرز ما فيه، وهي شبكة الإنترنت واستخداماتها الحديثة كالتجارة الإلكترونية، ونتحدث فيه عن الواقع الافتراضي وتطبيقاته. ثم نخصص القسم الثاني من هذا الفصل للحديث عن ضعف ثقة الجماهير في أمن المعلومات على شبكة الإنترنت، والخطر المتزايد الذي تحمله التقنية على أمن هذه المعلومات.

في القسم الثالث نرصد أهم أربع مشكلات تؤثر على أمن المعلومات، وهي المشكلات التي ظهرت مع ظهور شبكات المعلومات وانتشارها.

نختم الفصل بإظهار مدى حاجتنا إلى بيئة معلوماتية آمنة، وإلى خمسة عناصر محددة يجب أن تتوافر في هذه البيئة، حتى تنجح مشروعات التجارة الإلكترونية والحكومة الإلكترونية وغيرها من المشروعات التي يعتبر أمن المعلومات هو عصب نجاحها.

١ـ١ عصر المعلومات:

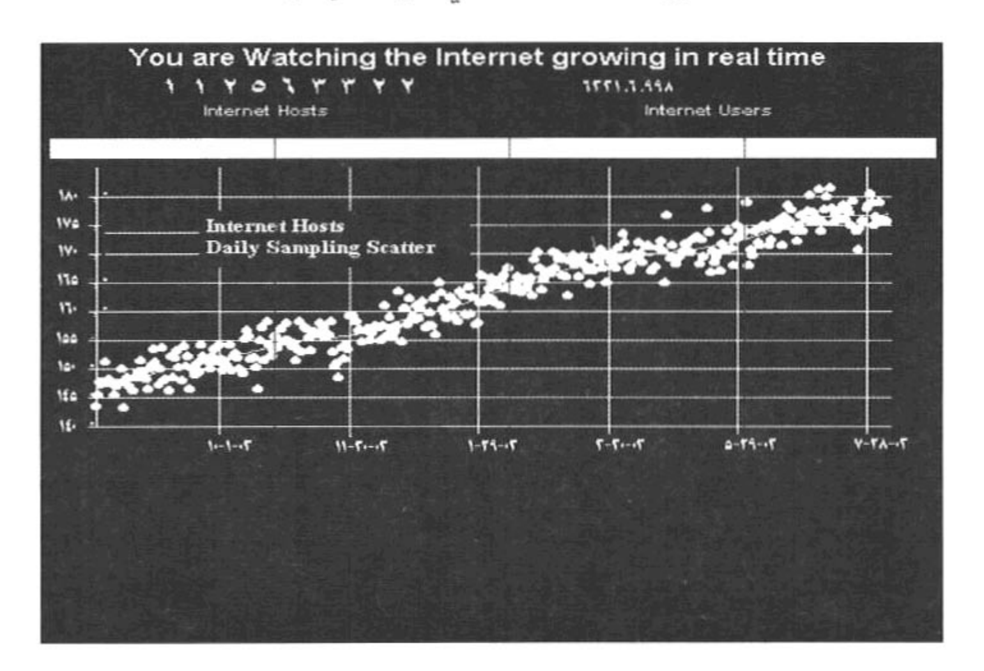
ربما كان من أهم السمات التي تميز العصر الذي نعيشه، في العقد الأول من القرن الحادي والعشرين، هو ازدياد المعلومات من حولنا، وازدياد استخدامنا لهذه المعلومات، وازدياد اعتمادنا عليها في حياتنا اليومية. ويتمثل ذلك بصورة جلية في نمو شبكة الإنترنت، وتزايد الاعتماد على البريد الإلكتروني، وتزايد المواقع التي تقدم خدماتها على الشبكة العالمية.

١-١-١ نمو شبكة الإنترنت:

التزايد الذي نلحظه في استخدام شبكة الإنترنت يفوق كل تصور، ففي اللحظة التي يكون فيها هذا الكتاب بين يدي القارئ الكريم سيكون عدد مستخدمي شبكة الإنترنت في العالم قد تجاوز نصف مليار مستخدم! فوفقاً لإحصاءات موقع (Internet Sizer) على شبكة الإنترنت [Internetsizer ٢٠٠٣] والموضحة في شكل (١-١) فإن عدد مستخدمي شبكة الإنترنت في أغسطس ٢٠٠٣م بلغ ٦٣٣,١٠٦,٩٩٨ مستخدماً، أي أكثر من نصف مليار من البشر يستخدمون هذه الشبكة. ويتضح من معدلات التزايد المنشورة على هذا الموقع أن عام ٢٠٠٥م سيشهد بلوغ عدد مستخدمي الشبكة مليار نسمة.

شكل (١-١)

تطور أعداد مستخدمي شبكة الإنترنت



يتبين من فحص إحصاءات المصدر نفسه أن عدد أجهزة الحاسب المستضيفة (Hosts) بالشبكة قد بلغ ١٨٠,٢٥٢,٠٠٠ حاسب، أي مائة وثمانين مليون جهاز بنهاية شهر نوفمبر ٢٠٠٣م كما يبدو في جدول (١-١).

جدول (١-١)

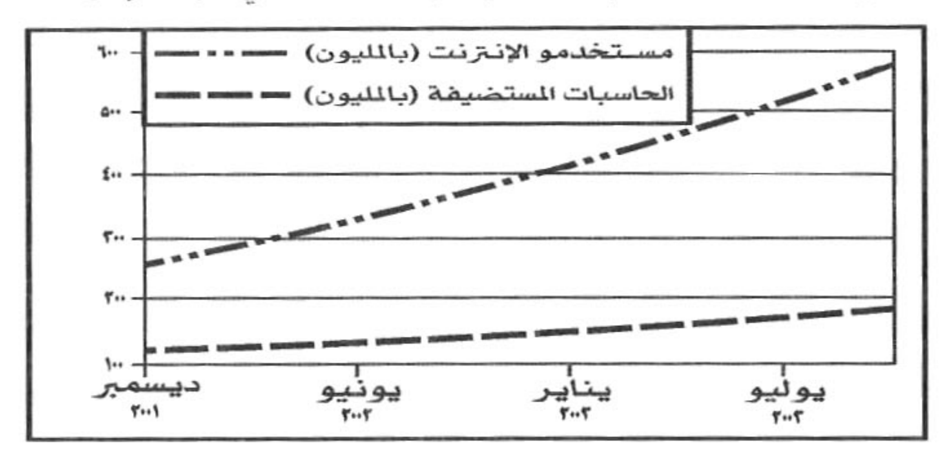
متوسط أعداد الأجهزة المستضيفة شهريًا خلال السنوات الثلاث الأخيرة

	٢٠٠١	٢٠٠٢	٢٠٠٣
يناير	١٠٠,٤٦٤	١٣٢,١٢٢	١٥٨,٠٠١
فبراير	١٠٣,٩٥٩	١٣٤,٣٤٧	١٥٩,١١١
مارس	١٠٧,١٨٧	١٣٦,١٧٧	١٦٢,١٢٧
أبريل	١٠٩,٨٢٨	١٣٩,٠٣٥	١٦٤,٩٤٣
مايو	١١٢,٠٧٢	١٤٠,٣١٥	١٦٧,٠٠٥
يونيو	١١٤,٨٠٤	١٤٢,١٢١	١٦٩,١٦٨
يوليو	١١٧,٢٨٨	١٤٥,١١١	١٧١,٢٩٧
أغسطس	١١٩,٢٠٧	١٤٧,٣٢٣	١٧٢,٥٢١
سبتمبر	١٢٢,١٧٧	١٥٠,١٨٩	١٧٤,٦١٢
أكتوبر	١٢٤,٤٤٣	١٥٣,١٥٢	١٧٧,٠٠٧
نوفمبر	١٢٧,٢٣٣	١٥٥,١٣٧	١٨٠,٢٥٢
ديسمبر	١٣٠,٤٤٢	١٥٦,٩٨٤	

وبتحليل الإحصاءات الواردة في هذا الموقع يتبين أن نمو هذه الأجهزة يتم بمعدل ٣,٥٪ شهريًا، أو أن عددها يتضاعف تقريبًا كل ثمانية عشر شهرًا. أي أن هناك أكثر من ثلاثة ملايين ونصف مليون جهاز تتم إضافتها للشبكة كل شهر. وإذا استخدمنا المعدل المبين في الجداول المنشورة على هذا الموقع وفقًا لبيانات الشهور الأخيرة من عام ٢٠٠٣م، نجد أن معدل انضمام أجهزة الحاسب المستضيفة (Hosts) إلى شبكة الإنترنت هو ٨٠ جهازًا كل دقيقة!

ويبين شكل (١-٢) نمو عدد أجهزة الحاسب المستضيفة من ١٢٠ مليون جهاز إلى نحو ١٨٠ مليون جهاز وعدد مستخدمي شبكة الإنترنت من نحو ٤٢٠ مليون مستخدم إلى نحو ٦٣٠ مليون مستخدم وذلك خلال ١٨ شهرًا فقط، كما يظهرها موقع (Telcordia) على شبكة الإنترنت [Telcordia ٢٠٠٣]. وإذا علمنا أن عدد سكان العالم حاليًا هو حوالي ستة مليارات نسمة، لذلك فليس من المستغرب أن نقبل في المستقبل القريب على وضع يصبح فيه كل شخص في العالم مرتبطًا بالإنترنت بصورة أو بأخرى. وهذا هو ما تراهن عليه شركات تقديم خدمات الحاسب في العالم، وما تراهن عليه حكومات الدول التي بدأت تخطو خطوات جادة وواسعة نحو مشروع " الحكومة الإلكترونية " لتقديم خدماتها لمواطنيها عبر شبكة الإنترنت.

شكل (١-٢)
نمو عدد أجهزة الحاسب المستضيفة وعدد مستخدمي شبكة الإنترنت



١-١-٢ نمو البريد الإلكتروني:

كان البريد الإلكتروني من أقدم وأهم استخدامات الشبكة، وربما ترجع بدايات استخدام البريد الإلكتروني إلى العام ١٩٨٠م عندما بدأت بعض شركات الحاسب (ربما كان السبق لشركة صن ميكروسستمز) إعداد قوائم البريد الإلكتروني للاتصال بعملائها، كما بدأت شركات الحاسب وغيرها من الشركات بتقديم خدمات الدعم الفني لعملائها عبر شبكة الإنترنت. وهكذا اقتحمت الإنترنت مجال التجارة والمال والأعمال من أوسع الأبواب.

سرعان ما تبين للشركات أن هناك مجالاً ممتازًا لتوفير النفقات وتحسين الخدمة، فبدلاً من أن ينتظر العميل على الهاتف حتى يفرغ له الموظف المختص ليقدم إليه المساعدة الفنية المطلوبة، فإن هذا العميل يستطيع أن يرسل للشركة بريدًا إلكترونيًا يشرح فيه المشكلة التي تواجهه، وينتظر الرد بالبريد الإلكتروني أيضًا. وهكذا انخفضت النفقات (بالتوفير في أجور المكالمات الهاتفية)، وتحسنت الخدمة المقدمة للعملاء. ومن جهة أخرى فإن المشكلة، إذا استعصى حلها على الموظف الذي استقبلها، فهو يستطيع بسهولة أن يحيلها (Mail forwarding) إلى شخص آخر

أقدر على حلها، مرفقاً كل البيانات التي حصل عليها من العميل. كما يمكن أن يتم الرد على العميل عن طريق إحالته إلى موقع آخر قد يجد فيه حلاً لمشكلته.

١-١-٣ تزايد المواقع على الشبكة العالمية:

بانتشار استخدام البرامج المستعرضة (Browsers) والقدرة على استعراض محتويات المواقع المختلفة على الشبكة، توسعت خدمات شبكة الإنترنت بشكل هائل، من خلال قيام الشركات والمؤسسات ومقدمي الخدمات المختلفة بإنشاء مواقعهم على الشبكة. ونرى تزايد عدد المواقع على الشبكة بمعدل يقارب ١٨٪ في الشهر الواحد [Grant ١٩٩٨]، وتنوعت الخدمات التي يتم تقديمها من هذه المواقع لتغطي مجالات عديدة، ودخلت في نسيج المجتمع حتى أصبحت ركناً أساسياً يعتمد عليه كثير من البشر في تصريف أمور حياتهم اليومية.

١-١-٤ الحياة الرقمية:

بدأ الإنسان ينتقل إلى الحياة الرقمية بعد أن دخلت التقنيات الرقمية إلى كل مجالات حياته، سواء في وسائل الاتصال مع الآخرين، أو الاتصال مع الآلة. وبدأنا نسمع عن التجارة الإلكترونية (Electronic Commerce)، والحكومة الإلكترونية (Electronic Government) وساعدت تقنيات الاتصالات وأنواع الشبكات الرقمية الجديدة فائقة السرعة (التي سنتحدث عنها في الفصل الثالث من هذا الكتاب) على زيادة اعتماد الإنسان على هذه الحياة الرقمية، فسمح لها بالدخول إلى جميع مجالات حياته. فعندما اكتشفت البنوك فوائد شبكة الإنترنت، وعندما تنبه العاملون في صناعة البنوك إلى الأهمية الإستراتيجية للتجارة الإلكترونية ودور البنوك فيها، بدأ منذ عام ١٩٩٦م انتشار المواقع الجديدة للبنوك على الشبكة، وكان ذلك بمعدل ١٢ بنكاً جديداً في كل أسبوع واستمر هذا التصاعد حتى الآن حيث انتشرت " البنوك الإلكترونية " (Electronic banking).

١-١-٥ الواقع الافتراضي (Virtual reality):

بانتشار الحاسبات فائقة السرعة وظهور إمكانيات العرض المتطورة أصبح من الممكن عرض صور متتابعة ثلاثية الأبعاد على شاشة الحاسب، وتحريكها بمعدل سريع جدًا يجعلها تبدو للمشاهد كما لو كانت تتحرك بشكل طبيعي مجسم. ثم تطور مفهوم " الواقع الافتراضي " (Virtual reality) فقدمت شركة " فورد " مؤخرًا عرضًا لتصميم إحدى سياراتها على شاشة حاسب عملاقة استوعبت صورة السيارة بحجمها الطبيعي. وبدت السيارة للمشاهد مجسمة في الهواء، بحيث تظهر جميع تفاصيلها بدقة وهي بارزة في الفراغ الموجود أمام الشاشة، وذلك باستخدام أسلوب " الواقع الافتراضي ".

ظهرت كذلك " الشبكات الخاصة الافتراضية " (VPN) - والتي سنتناولها بالتفصيل في الفصل العاشر من هذا الكتاب - لتحقق عنصر الأمن المفقود على الشبكة. ودخلنا عالمًا " افتراضيًا " جديدًا مثلما دخلنا العالم " الرقمي " من قبل، فظهرت الجامعات الافتراضية (Virtual universities) التي لا يعرف الدارس فيها أين تقع، ولا يهمه ذلك، ولكنه يدرس فيها ويحضر المحاضرات ويؤدي الاختبارات، بل يتوجه بأسئلته إلى " المدرس الافتراضي ". وهناك مشروع يدعمه الاتحاد الأوروبي حاليًا لإنشاء جامعة افتراضية عالمية، وتشترك في هذا المشروع إحدى عشرة دولة، ويتوقع الانتهاء من هذه الجامعة الجديدة في العام ٢٠٠٤م.

ودخلت التقنية الافتراضية عالم الإنشاءات باستخدامها في تصميم المباني وتعديل هذا التصميم مرة تلو الأخرى حتى يصل المبنى المصمم إلى مرحلة القبول الكامل من أصحاب القرار.

١-١-٦ تطور التجارة الإلكترونية:

من المؤكد أن أنشطة التجارة الإلكترونية تتطور بشكل ملحوظ، وكانت التوقعات في بداية ظهورها طموحة جدًا، ففي دراسة أجرتها مجموعة " يانكي " (Yankee Group)

في عام ١٩٩٥م أن السوق الأفقية للتجارة الإلكترونية من المتوقع أن تستمر في النمو إلى أن يصل حجمها إلى ١٣٤ مليار دولار في عام ٢٠٠٠م [Vinet ١٩٩٦] وتوقعت هذه الدراسة أن هذا النمو سيتحقق من خلال زيادة عدد الصفقات التي تتم على الشبكة من ١٥٠,٠٠٠ صفقة في عام ١٩٩٥م إلى حوالي ملياري صفقة في عام ٢٠٠٠م، ومما دعم هذه التوقعات في ذلك الوقت قيام شركة (DEC) وحدها في عام ١٩٩٦ بعقد صفقات تربو قيمتها على ٢٣٥ مليون دولار من خلال شبكة الإنترنت (Hamilton ١٩٩٧).

ولكن يلزم أن نبين أن المتابع لانتشار التجارة الإلكترونية يجد أن هذا الانتشار لم يتم بالفعل بنفس التوقعات الطموحة التي صاحبت ظهور مشاريع التجارة الإلكترونية وبداياتها الواعدة. وأعتقد أن قصور تقنيات أمن المعلومات، وتردد جمهور المتعاملين من خلال شبكة الإنترنت في الإقبال على أنشطة التجارة الإلكترونية لضعف ثقتهم في إجراءات الأمن، يقفان وراء هذا التباطؤ الذي يجعلنا نتحفظ مع ما يطالعنا به المختصون من توقعات متفائلة.

١-١-٧ انتشار استخدام شبكة " الإنترانت "(Intranet):

اكتشفت كثير من الشركات أن التقنية التي تستخدمها في استعراض مواقع الشبكة، وكذلك التقنيات المستخدمة في أجهزة الخدمة التي تربط الشركة بالعالم الخارجي من خلال شبكة الإنترنت، يمكن أن تستخدم هي نفسها لربط شركتهم مع فروعها المختلفة أو مع الشركات المتعاملة معها. وكان لهذا الاكتشاف أثره العميق على شبكات المعلومات الداخلية في المؤسسات والشركات المختلفة، حيث تم تطبيق نفس التقنيات المستخدمة في شبكة الإنترنت، ونشأ بذلك ما نطلق عليه " الإنترانت ". وسنتعرض لشبكة الإنترانت عند حديثنا عن شبكات المعلومات في الفصل الثالث من هذا الكتاب.

ولنأخذ مثلاً شركة الاستثمار " مورجان ستانلي "، التي يستخدم موظفوها البالغ

عددهم عشرة آلاف موظف شبكة الإنترانت بشكل مستديم. كان مقدار التوفير الذي تحقق للشركة في عملية توزيع المعلومات على موظفيها باستخدام الإنترانت، مقارنة باستخدام الأساليب الورقية من قبل، بين ٣٠٠,٠٠٠ دولارًا و ٧٠٠,٠٠٠ دولارًا سنويًا. وفي الشهور الثمانية عشر الأولى لتشغيل شبكة الإنترانت في الشركة حققت الشركة توفيرًا فعليًا في النفقات قدره مليون دولار (Kambil ١٩٩٧).

من بين خدمات الإنترنت المميزة التي استعارتها الإنترانت، خدمة البريد الإلكتروني (Email)، وخدمة " تصفح المواقع " .(Site Browsing) وتلجأ شركات كثيرة إلى استخدام هذه التقنيات في شبكاتها الداخلية، حتى يظل موظفو هذه الشركات على علم بما يدور في شركاتهم أولاً بأول. كما تجعل قوائم البريد الإلكتروني الموظفين الذين يعملون في مواقع بعيدة يقفون أولاً بأول على أحدث التطورات وآخر المنتجات التي تنتجها شركتهم، أو أي تغيير يطرأ على الأسعار، كما يقفون من خلالها على الموقف التنافسي للشركة. بل وتستطيع الشركة أن تدرب موظفيها على استخدام منتجاتها من خلال ما يسمى بالتدريب عن طريق الشبكة (Web-based training) وفي نفس السياق لم يعد وجود الكتالوجات الإلكترونية المستخدمة في التسويق أمرًا غريبًا على شبكة الإنترنت هذه الأيام.

نتج عن كل هذا التطور في الخدمات، وعن الاستخدام المكثف للتقنيات، انخفاض هائل في تكلفة الخدمات التي تقدم للمستهلك. وأصبح من السهل على الشركات، عن طريق استخدام بعض المواقع على الشبكة، تقديم دورات تدريبية كاملة لموظفيها أو لعملائها المنتشرين على اتساع العالم كله، مع متابعة تقدمهم ورصد نتائجهم.

١ - ٢ أمن المعلومات:

هذا التوسع الكبير في تبادل المعلومات وانتقالها من مكان إلى آخر أنشأ هاجسًا لم يكن بهذه الحدة من قبل.. أعني به هاجس الأمن، أمن سلامة هذه المعلومات والمحافظة على تكاملها، وعلى وصولها سليمة للشخص المعني وحده دون غيره.

ولأن التقنيات المستخدمة في شبكات إنترانت الداخلية هي نفسها التي تستخدم في شبكة الإنترنت، فإن المشاكل التي تعاني منها الإنترانت هي نفسها المشاكل التي ورثتها عن الإنترنت، كما أن حلول هذه المشاكل تنطبق في كلتا الحالتين، وقد زاد كل ذلك من أهمية موضوع الأمن.. أمن المعلومات على كلا المستويين؛ فبازدياد حجم ودرجة تعقيد الخدمات المقدمة، سواء من خلال الإنترنت أو الإنترانت، فالحاجة إلى إثبات الشخصية وإلى توفير الخصوصية وسرية المعلومات أصبحت أكثر إلحاحًا من ذي قبل. فعندما كان استخدام الشبكة قاصرًا على أغراض التسويق فقط، لم يكن لأمن المعلومات الأهمية الكبيرة التي يتمتع بها الآن، لأن المعلومات كانت متاحة للجميع وبلا قيود. أما بعد توجه الشركات إلى استخدام الشبكة في قطاع الأعمال وعقد الصفقات والتجارة الإلكترونية، فإن ما كانت أهميته محدودة في السنوات الأخيرة من القرن الماضي أصبح عظيم الأهمية مع بدايات القرن الحالي.

توجد على شبكة الإنترنت بعض المواقع الهامة التي تعني بأمن المعلومات وننصح القارئ باللجوء إليها للحصول على المزيد من المعلومات الأمنية المفيدة وهي :

(١) موقع CERT Coordination center وعنوانه http://www.cert.org

(٢) موقع معهد SANS للأمن وعنوانه http://www.sans.org

١-٢-١ الثقة في أمن شبكة الإنترنت:

برغم مضي وقت طويل على انتشار استخدام شبكة الإنترنت، إلا أن مستخدمي الإنترنت لا يثقون كثيرًا في أمن هذه الشبكة. فهم يخشون عند استخدام بطاقات الائتمان الخاصة بهم على شبكة الإنترنت أن يحصل طرف ثالث على أرقام هذه البطاقات، ويشتري سلعًا باستخدامها، أو ربما يستغلها في السحب من أرصدتهم في البنوك. كما يخشى مستخدمو الشبكة مما يمكن أن يترتب على شراء البضائع من المواقع المختلفة على الشبكة، خوفًا من أن تكون هذه المواقع مواقع زائفة. كما أنهم يخشون كذلك من اكتشاف الآخرين لكلمة السر التي يستخدمونها عند التعامل مع

البنوك، فيساء استخدام حساباتهم. كما ينتاب القلق دوائر الحكومة والعاملين في قطاع الأعمال، وقطاع البنوك على وجه الخصوص، من احتمال إفشاء بعض المعلومات الحساسة لأطراف غير مخولة بالحصول عليها. وفي الإطار نفسه تخشى الشركات من تسرب المعلومات الحساسة لبعض الموظفين الذين ربما لا يكونون مخولين بالاطلاع عليها، أو ممن يحاولون التلصص على بيانات زملائهم. كما تخشى كثير من المؤسسات من حصول منافسيها على معلومات داخلية، مما قد يسبب الحرج للمؤسسة، أو يحرمها من ميزة المنافسة.

برغم أن المتعاملين مع الإنترنت يميلون إلى إجمال كل هذه الوساوس والمخاوف والرغبة في تجاوزها في مصطلح واحد هو " الأمن "، إلا أن هناك في الحقيقة مصطلح أكثر شمولاً ووضوحاً، وأميل شخصيًا لاستخدامه، وهو مصطلح " الأمان ". وبالأمان نعني أن أي شيء سواء كان ملفًا أو معلومة أو نظامًا أو جهاز اتصالات يجب أن يكون محميًا ضد أي استخدام غير مشروع أو أي تعديل من جانب طرف غير مخول بذلك.

وهكذا يعبر مصطلح " الأمان " عن البيئة الآمنة وعن نتائج التأمين وعن التأكد من سلامة إجراءات أمن المعلومات، وبذلك يعتبر أكثر شمولاً من مصطلح " الأمن ".

١-٢-٢ الزيارات العدائية للمواقع:

تشهد صناعة المعلومات، من آن لآخر، عمليات اقتحام عديدة، أو ما يمكن أن نطلق عليه (الزيارات العدائية) لمواقع المؤسسات على شبكة الإنترنت. وقد أدخلت هذه الممارسات العالم في أشكال جديدة من الصراعات الإلكترونية الشرسة التي تتم بواسطة محترفين، ولم تعد قاصرة على هواة الاقتحام أو هواة التسلل إلى المواقع. ومن المتوقع أن تستمر هذه الصراعات وتتطور بصورة سريعة وحادة في مباراة شرسة بين خبراء أمن المعلومات الذي يسعون للدفاع عن المعلومات وعن المصالح الاقتصادية التي تتوقف على أمن هذه المعلومات، وبين أطراف تسعى إلى ضرب هذه المصالح من

خلال شبكة الإنترنت محدثة خسائر تقدر بملايين الدولارات. والمتوقع أن تصل هذه الخسائر إلى مليارات الدولارات في وقت قريب مع تزايد الاعتماد على شبكة الإنترنت في التجارة الإلكترونية. ومستقبل هذا النوع من التجارة مرهون بقدرة خبراء الكمبيوتر على استحداث أنظمة حماية جديدة قادرة وفعالة ضد العبث الإلكتروني بأمن المعلومات.

وقد شهد شهر فبراير ٢٠٠٠م اعتداءات متكررة على عدد من مواقع التجارة الإلكترونية لشركات عالمية كبرى على شبكة الإنترنت، وقد أسفرت هذه الاعتداءات عن تحقيق خسائر فادحة لهذه الشركات. وتعرضت لهذه الاعتداءات مواقع شبكة " سي إن إن " الإخبارية، وشركة " أمازون " لتوزيع الكتب، وموقع " ياهو " الشهير، وغيرها من الشركات الأمريكية واليابانية. وقد أعلنت مؤسسات خليجية مالية عن تعرض مواقعها على الإنترنت لبعض الزيارات العدائية التي أنتجت خسائر متفاوتة. وهؤلاء المعتدون ليس من المعتقد أنهم أفراد مستقلون، بل هم في الغالب يعملون ضمن جماعات منظمة، أو ربما تجمعهم وتنظمهم وتعينهم دول معينة على أداء مهامهم التخريبية. ويلزم لذلك تطوير الدفاعات الحالية مثل " جدران الحماية " (Firewalls) وغيرها لصد محاولات الاقتحام هذه.

لكي نتفهم ما حدث في فبراير ٢٠٠٠م من هذه الزيارات العدائية، فإننا يمكن أن نصنفه كنوع من " عرقلة الخدمة " (Denial of Service)، وكان يستهدف إيقاف هذه المواقع عن العمل من خلال استخدام أسلوب " التحميل الزائد " (Overloading) للموقع لعرقلة أدائه لعمله، وجعله عاجزًا عن استقبال طلبات الشراء والبيع وغيرها. فإذا كان الموقع مصممـًا لاستقبال ألف رسالة في الدقيقة مثلاً فيتم إرسال ١٠٠ ألف رسالة إليه، أو شغله بشكل متصل باستفسارات متوالية تتطلب الإجابة عنها فترات زمنية طويلة، مما يوقف هذا الموقع كليًا عن العمل، الأمر الذي يحقق خسائر مادية للشركة. وربما كان أهم من هذه الخسائر المادية الخسائر غير المادية، مثل ضعف ثقة العملاء.

١-٢-٣ الخطر الأمني المتزايد على المعلومات:

كانت التجارة الإلكترونية هي أكثر المتضررين وأكثر المستهدفين من الزيارات العدائية التي تحدثنا عنها، ويبدو هذا واضحًا من اختيارات المهاجمين التي أكدت أن وراءها دوافع اقتصادية. والأمر الذي يجب أن نلفت إليه الانتباه هو أننا قد بدأنا بالفعل نواجه عمل المحترفين، وليس الهواة. وهؤلاء المحترفون يسعون بشراسة لإلحاق الأضرار الاقتصادية بكثير من الشركات. ونتوقع أن يستمر هذا الاتجاه في التصاعد، مما يفرض على خبراء أمن المعلومات أن يصعِّدوا بدورهم من وسائل الحماية وتقنياتها. ويفرض ذلك أيضًا على الدول أن تنظر إلى الموضوع بشكل أكثر جدية. وما زلنا نذكر ظهور وزيرة العدل الأمريكية في ١٩ مايو ٢٠٠٠م على شبكات التلفزة العالمية لتعلن عن ظهور فيروس جديد، وتعقد مؤتمرًا صحفيًا يشرح فيه خبراء مكتب التحقيقات الفيدرالي (FBI) كيفية عمل الفيروس ووسائل انتقاله. ولعل هذا الاهتمام يلفت انتباهنا إلى أن العالم ينظر بكل الجدية والاهتمام لأمن المعلومات. وأود هنا أن أدعو الدول العربية لكي تنشيء كل دولة إدارة عامة لأمن المعلومات في إحدى الوزارات التي تهتم بالأمن أو التي تهتم بتقنيات المعلومات، بحيث تكون مهمة هذه الإدارة متابعة كل جديد في مجال تقنيات أمن المعلومات، ودراسة الأخطار التي تهدد أمن المعلومات في وزارات الدولة وفي قطاعيها العام والخاص، وتقديم الحلول الجاهزة، وتنمية الخبرات في هذا المجال، وتنظيم الدورات التدريبية سواء للمتخصصين في أمن المعلومات أو للمستفيدين العاديين من أجل زيادة وعيهم الأمني في هذا المجال. كما يجب أن تسرع الدول العربية في إعداد التشريعات القانونية اللازمة لردع المعتدين وعقابهم درءًا لخطرهم. فالتشريعات الحالية غير كافية، أو هي غير شاملة، أو هي في كثير من الأحيان غير موجودة!

١-٣ أثر شبكات المعلومات على أمن المعلومات:

بظهور شبكات المعلومات زادت المخاطر الأمنية التي تتعرض لها المعلومات، كما أن

هناك خصوصية للأمن في عالم الشبكات جعلت من الضروري أن ننظر إلى أمن شبكات المعلومات بشكل أكثر جدية وصرامة. فالشركات الآن في حوارها مع فروعها لا تضمن عدم وجود (طرف ثالث) يتنصت على هذا الحوار، فالمعلومات المتبادلة تمر عبر عشرات الدول وملايين الحاسبات والكابلات، وبعض هذه الكابلات أرضي أو بحري أو حتى فضائي، فهناك دائمًا الخشية من وجود هذا (الطرف الثالث). وقد يهون الأمر إذا اقتصر تدخل الطرف الثالث على التنصت، بل إنه ربما يقوم بتغيير الرسائل المتبادلة، فيتدخل في طلب شراء البضائع المقدم من العميل لشركة لتوريد البضائع، فيضع عنوانه هو مكان عنوان طالب الشراء، فيتم إرسال البضائع إلى عنوان المجرم. أو قد يغير المجرم رقم الحساب البنكي المحول إليه مبلغ ما إلى حساب بنكي آخر. لذلك تظهر بشدة أهمية " التحقق من الشخصية " (Authentication) لأمن التعامل عبر شبكة الإنترنت، وهذا ما سنتعرض له في الفصول التالية من هذا الكتاب.

هناك مشكلات أمنية أساسية في عالم شبكات المعلومات هي:

- عدم التواجد المباشر.
- سهولة النسخ والتعديل.
- الأنشطة الآلية.
- شيوع التواجد.

وسنتعرض فيما يلي لهذه المشكلات وأثرها على أمن الشبكات.

١-٣-١ عدم التواجد المباشر:

بسبب عدم وجود تواجد فعلي أو مباشر للأشخاص على الشبكة، فإن كثيرًا من وسائل الأمن المستخدمة في حياتنا اليومية لا يمكن تطبيقها على الشبكة. وينطبق ذلك على خمسة عناصر للأمن وهي: التحقق من الشخصية، الترخيص بالاستخدام، الخصوصية وسرية المعلومات، صحة وسلامة البيانات، والثقة في المعلومات.

لأنه لا يوجد شخص فعلي نتحاور معه على الشبكة، تظهر مشكلة التحقق من شخصية الآخرين. فأنت مثلاً حين تريد التعامل مع البنك الذي تحتفظ لديه بحسابك الشخصي فأنت تذهب إلى مبنى البنك، وهذا المبنى تعرفه جيداً، وتستطيع التحقق من ذلك بسهولة. كما أنك تحمل بطاقة هوية تعرف بها نفسك لموظف الشباك، أي أن تعرف كل طرف على الآخر ممكن وسهل. أما في عالم الشبكات فأنت في حاجة للتأكد من أن الموقع الذي دخلت إليه على الشبكة هو بالفعل الموقع التابع للبنك الخاص بك. كما أن البنك، صاحب الموقع، يريد بدوره التأكد من أنك أنت بالفعل العميل صاحب الحساب.

١-٣-٢ سهولة النسخ والتعديل:

إذا أردت إعداد نسخة أخرى من وثيقة ما على الحاسب، فما أسهل ذلك، إذ بلمسة زر واحدة تستطيع إعداد نسخة أخرى. والنسخة في هذه الحالة، بعكس تصوير المستندات، تكون مطابقة تماماً للأصل، كلمة بكلمة وحرفاً بحرف. وإذا كان التحويل البنكي عبارة عن ملف إلكتروني، فكل ما يحتاج إليه المجرم للحصول على مزيد من المال هو نسخ هذا الملف أي عدد من المرات. ولأن التعديل سهل، فمن السهل تعديل مبلغ التحويل ليصبح أضعاف المبلغ الأصلي.

من السهل كذلك على أي شخص تعديل محتويات رسالة للادعاء بالباطل على مرسلها، وفي بعض النظم يصعب إثبات أن الرسالة قد تعرضت للتعديل. لذلك كله اكتسبت عملية الحماية ضد التعديل غير المرخص به أهمية كبرى في عالم شبكات المعلومات.

١-٣-٣ الأنشطة الآلية:

من السهل كتابة برنامج يقوم آلياً بمحاولة اقتحام بعض النظم، أو إرسال البريد الإلكتروني لآلاف المستفيدين (Spam mail)، أو سرقة الملفات، أو غير ذلك من وسائل

إساءة استخدام الشبكة. فإن أي شخص يستطيع نسخ برنامج رائع اسمه " كراك " (Crack) من على شبكة الإنترنت. هذا البرنامج يقوم بمقارنة كل كلمات السر بمحتويات قاموس اللغة الإنجليزية بحثًا عن تطابق كلمة السر بإحدى كلمات القاموس، وهي عملية سهلة، في الوقت الذي تكون فيه محاولة كسر الشفرة يدويًا أصعب بكثير.

١-٣-٤ شيوع التواجد:

على الشبكة يمكن افتراض وجود أي شخص في أي مكان، وكل شخص يمكن أن يدخل إلى الشبكة من أي دولة. فالشخص الذي عنوان بريده الإلكتروني مستمد من موقع (Hotmail.com) مثلاً يمكنه أن يرسل رسالة يذكر فيها أنه موجود في مدينة الرياض بينما هو في نيويورك مثلاً. ولقد كثر في الآونة الأخيرة أن بعض الشركات التي تطلب موظفين جددًا، ولا تريد الإفصاح عن نفسها أو عن مكان تواجدها، فإن هذه الشركة تذكر لنفسها عنوانًا مجهلاً مثل moc@hotmail.com ولا تعرف إن كان هذا العنوان (Moc) يخص " المركز العصري للكمبيوتر " في القاهرة (Modern Office for Computing) أو وزارة التجارة السعودية بالرياض (Ministry Of Commerce).

وبرغم أن الأشخاص غير متواجدين فعليًا على الشبكة، إلا أنهم (يفترض) وجودهم، وبالتالي فأنت تسكن بين جيران مجهولين، فأي شخص في العالم يمكن أن يكون جارًا مباشرًا لك. وأنت تستطيع أن تدخل إلى موقع يستضيفه جهاز في نفس المبني الذي تسكن فيه بنفس السهولة التي تدخل بها إلى أي موقع يقع في النصف الآخر من الكرة الأرضية.

لعل هذا هو السر في الجاذبية التي تتمتع بها شبكة الإنترنت، ولكنه أيضًا السر في الكثير من مشاكل الأمن على هذه الشبكة. صحيح أن جدران الحماية يمكن أن تساهم في الحد من هذه المخاطر، ولكن تظل هناك درجة معينة من الخطورة يظل يتعرض لها كل حاسب مرتبط بشبكة الإنترنت.

يمكن أن تنتج عن " شيوع التواجد " مشاكل قضائية على المستوى الدولي، فلو أن

شخصاً في " هونج كونج " قام بعملية تزوير نتج عنها سرقة أموال بنك في " بيروت "، فأي شرطة عليها أن تلاحقه؟ وأي سلطة قضائية يمثل أمامها إذا تم القبض عليه؟ وأي قانون يجب تطبيقه في هذه الحالة؟ بل أين هو مكان حدوث الجريمة؟ هل هو مكان تواجد المجرم؟ أم هو مكان تواجد المسروقات؟

١ ـ ٤ الحاجة إلى بيئة معلوماتية آمنة:

لكي نصل إلى تحقيق بيئة معلوماتية آمنة يلزم تحقيق عناصر الأمن التالية:

- التحقق من الشخصية Authentication
- الترخيص بالاستخدام Authorization
- الخصوصية وسرية المعلومات Privacy and Confidentiality
- صحة وسلامة البيانات Integrity
- الثقة في المعلومات Trust

هذه العناصر الخمسة تشكل المتطلبات الأساسية للأمن (أو الأمان) في شبكات المعلومات بصفة عامة، وليس فقط على الإنترنت. وتختلف درجة الأمان المطلوبة تبعاً لأهمية المعلومات المطلوب تأمينها، ومدى تعرض هذه المعلومات للخطر، وكذلك مدى الضرر الذي يخشى من وقوعه في حالة فقد واحد أو أكثر من هذه العناصر.

لنتحدث فيما يلي عن متطلبات الأمن الخمسة، وكيف يمكن تحقيقها للحصول على بيئة معلوماتية آمنة.

١ ـ ٤ ـ ١ التحقق من الشخصية (Authentication):

نحن نتعرف في كل يوم على شخصية الآخرين من البشر، كما نتعرف على شخصية الأماكن كذلك. نفعل ذلك بمطابقة صورة ما نشاهده مع ما تحتويه الذاكرة،

أو بمطابقة اسم الشارع مع العنوان المكتوب في الورقة التي نحملها، أو بمطابقة العلامة التجارية المرسومة على المتجر مع العلامة التي نعرفها جيداً. وفي البنك يتم التحقق من شخصية العميل عن طريق توقيعه.

في عالم الشبكات الأمر مختلف، فالتوقيع الكتابي لا يمكن استخدامه، والتحقق عن طريق الرؤية غير ممكن (بسبب عدم التواجد المباشر)، ولا يوجد دليل يثبت شخصية الموقع الذي يدخل إليه العميل، برغم ما قد يراه من علامات أو شعارات (Logos) في هذه المواقع. فالتقليد سهل والخداع أكثر سهولة، فافتعال موقع جديد مشابه للموقع الحقيقي، أو تسجيل اسم نطاق (Domain name) قريب من اسم الموقع يكاد لا يكلف شيئاً.

وسنتعرض في الفصول التالية للتوقيعات الرقمية (Digital signatures)وغيرها من أساليب التحقق من الشخصية في عالم الشبكات.

١-٤-٢ الترخيص بالاستخدام (Authorization):

تثبت رخصة القيادة صلاحية السائق لقيادة السيارة، وتثبت التأشيرة على جواز السفر حق المسافر في عبور الحدود. هذه الوسائل المستخدمة لإثبات الترخيص بالاستخدام (Authorization) تتطلب ثلاثة أمور:

١- وجود طرف ثالث يصدر الترخيص.

٢- الثقة في مقدرة الطرف الثالث على إصدار القرار السليم بمنح الترخيص.

٣- صعوبة نسخ أو تزوير أو تعديل هذا الترخيص.

هذا الطرف الثالث خارج عالم شبكات المعلومات قد يتمثل في وحدة تراخيص المرور، أو في إدارة الجوازات، أو نراه في الجامعات التي تمنح الشهادات الأكاديمية، أو في هيئة المواصفات والمقاييس التي تمنح شهادات الصلاحية أو المطابقة للمواصفات. وفي جميع هذه الأحوال نجد للطرف الثالث مقراً يتم التوجه إليه

للحصول على الترخيص، أو للتحقق من إصداره لهذا الترخيص، ونجد له موظفين يقومون بالتأكد من أحقية طالب الترخيص فيما يطلب.

أما في عالم شبكات المعلومات، فأين تذهب؟ وكيف يتم التعامل مع الطرف الثالث؟ وهنا يأتي دور تقنيات منح الصلاحيات "، وشهادات التعريف الرقمية "(Digital certificates).

١-٤-٣ خصوصية وسرية المعلومات (Privacy and Confidentiality):

المقصود بخصوصية المعلومات وسريتها هو التأكد من أن الطرف المعني هو وحده الذي لديه القدرة على الوصول إلى المعلومات. ونحن نحقق ذلك خارج عالم الشبكات باستخدام القفل والمفتاح، فدرج المكتب يفتحه مفتاح، وندير السيارة بمفتاح، ونراجع بريدنا في صندوق البريد بمفتاح. وتكون هذه المفاتيح من النوع المفرد(Symmetric)، أي أن المفتاح المستخدم في الإغلاق هو نفسه المستخدم في الفتح. وفي خزائن البنوك مثلاً هناك مفتاحان يحمل أحدهما أحد موظفي البنك، والآخر يحمله العميل، ولا يمكن فتح الخزانة إلا باستخدام المفتاحين معًا. وحيازة العميل للمفتاح تعني " الترخيص بالاستخدام "، فمن يحصل على المفتاح يستطيع الدخول حتى لو كان لصًا أو شخصًا استطاع سرقة المفتاح ثم إعداد نسخة مزورة منه. وإن كانت سرقة المفتاح خارج عالم الشبكات قد تلفت نظر الضحية فيمكنه تغيير القفل مثلاً، أما في عالم الشبكات فقد يحصل الآخرون على مفاتيحك دون أن تشعر وهذا الأمر سهل جدًا ووارد جدًا. كل من هذه الأساليب (والمفاتيح) لها ما يقابلها في عالم الشبكات كما سنرى لاحقًا.

خارج عالم الشبكات فإن إغلاق المظروف بخاتم معين يعتبر ضمانًا أن هذا المظروف لم يتم فتحه من قبل طرف دخيل، و السياج العالي حول المنزل يعتبر ضمانًا وحماية من تلصص الآخرين وانتهاكهم للخصوصية والسرية. وفي عالم الشبكات يضمن تشفير الملفات والرسائل حماية مماثلة لها، فلن يستطيع الاطلاع على الملفات إلا حامل مفتاح فك الشفرة. وهناك أيضًا " التوقيعات الرقمية "، و" النفق الآمن "(Secured tunnel).

يتم خارج عالم الشبكات مراقبة الأصول الثمينة بواسطة الكاميرات السرية في

البنوك أو المتاجر أو المتاحف، كما تستخدم في ذلك أجهزة الاستشعار المختلفة، وكلما ازدادت أهمية الأصول المطلوب حمايتها تعددت الحواجز وازداد تعقيدها. الأمر نفسه يتم في عالم شبكات المعلومات، فالمراقبة مهمة جداً، كما يتم فحص الشبكة بأجهزة الفحص (Scanners) للتأكد من إجراءات الأمن، كما تتم متابعة التقارير التي يخرجها الحاسب. وفي عالم الشبكات تتعدد الحواجز كذلك ويزداد تعقيدها بازدياد أهمية الأصول المطلوب حمايتها، وسوف نرى في الفصول القادمة كيف يمكن تنفيذ ذلك كله.

١-٤-٤ صحة وسلامة البيانات(Data Integrity):

يمكن التأكد من صحة البيانات وسلامتها خارج عالم الشبكات بالأختام والتغليف الذي لم يتم فضه، وحتى في حالة فض الرسالة بواسطة إحدى الجهات الرقابية مثلاً كالجمارك، فإن هذه الجهة تعيد تغليف الرسالة وختمها حتى لا يشك مستقبل الرسالة في سلامة ما بها. أي أن التغليف والأختام هي وسيلة للتأكد من صحة وسلامة الرسائل والبضائع. ويتم التأكد من ذلك عادة عن طريق التحقق بالنظر لإثبات عدم وجود علامات دالة على انتهاك المغلف. حتى في العقود التي تتم بين طرفين، فإن أي تعديل في بيانات العقد المطبوع لابد من أن يصحبه توقيع الطرفين للدلالة على أن هذا التعديل قد تم بواسطة طرفي العقد.

في عالم الشبكات نضطر لفعل الشيء نفسه، وإن كان الأمر أكثر صعوبة بسبب سهولة نسخ البيانات وتعديلها، وبسبب شيوع التواجد على الشبكة. لذلك تستخدم "الأغلفة الرقمية "(Digital Envelopes)، كما نلجأ إلى طرف ثالث لتأكيد شخصية الأطراف التي نتعامل معها على الشبكة مثل " سلطة منح الشهادات الرقمية " (Certification authorities).

١-٤-٥ الثقة في المعلومات(Trust):

ربما كان عنصر الثقة في دقة وصحة المعلومات هو العنصر المشترك الذي يجمع

باقي العناصر الأربعة السابقة. هذا العنصر وجوده ضروري ومحتم، وإلا انهار الأمن، حتى مع توافر العناصر الأخرى. فأنت إذا لاحظت أن الكرسي الذي تنوي الجلوس عليه غير ثابت فإنك لن تقدم على الجلوس. وفي عالم الشبكات، لو شعر العميل بأن الآليات المستخدمة في شبكة معلوماته ليست بالكفاءة التي تضمن إثبات شخصية الموقع الذي يدخل إليه، أو شخصية الأشخاص الذين يتعامل معهم، أو لا تضمن قيوداً وشروطاً للترخيص باستخدام الملفات التي تحتوي على بياناته المالية، أو لا تضمن خصوصية وسرية المعلومات التي يدخلها العميل عن نفسه أو عن شركته، أو صحة وسلامة البيانات التي يحصل عليها من الموقع الذي يزوره. لو شعر العميل بالشك في توافر هذه العناصر، أو أنها لا تتوافر بالمستوى المطلوب، فإنه سوف يتردد في استخدام هذه الشبكة. مما يعني أن العميل لابد أن (يطمئن) إلى سلامة هذه العناصر، ولا يتأتى ذلك إلا بأن تكون كيفية تحقيقها واضحة له وظاهرة أمامه، وأن يستطيع اختبارها بنفسه والتحقق من عناصر أمن المعلومات في أي لحظة، أي المزيد من الشفافية. ومن مشاكل عالم الشبكات في هذا المجال أن هذه الثقة تتطلب مستوى معيناً من المعرفة لدى العميل، أو حداً أدنى مما يمكن أن نطلق عليه (ثقافة الكمبيوتر)، أو على الأقل ثقافة الإنترنت. وهذه الثقة من جانب الجماهير هي أهم عامل يمكن أن يؤثر في نجاح وانتشار التجارة الإلكترونية، أو فشلها وانحسارها.

يثق المريض في طبيبه لأنه تعامل معه من قبل، ويثق صاحب السيارة في الميكانيكي لأنه قام عدة مرات بإصلاح سيارته بكفاءة. ولكن عند دخول المريض إلى عيادة طبيب جديد لا يعرفه، أو عند دخول صاحب السيارة إلى ورشة ميكانيكي لم يسبق له التعامل معه، فهناك حاجة إلى ما يشجعه على منح الثقة المطلوبة. وربما كانت توصية صديق (طرف ثالث) مفيدة في هذا المجال، فهو قد يمتدح الطبيب أو الميكانيكي، وقد تكون شهادة هذا الصديق أفضل من شهادة الدكتوراه المعلقة في إطار على حائط غرفة الانتظار في عيادة الطبيب. وربما كان ازدحام ورشة الميكانيكي بالعملاء هو العامل المطمئن. والثقة مطلوبة بدرجة أكبر عند إيداع الأموال في البنوك، فيهم العميل أن يثق

في أن لدى هذا البنك خزائن قوية ضد السرقة، وأن بياناته لا يمكن تعديلها أو التلاعب فيها. كما يهمه أن يطمئن إلى المركز المالي للبنك. وفي عالم الشبكات يوجد الطرف الثالث " سلطات منح الشهادات الرقمية "، وتوجد " جدران الحماية "، و" خوادم البروكسي "، و" أجهزة كشف الاقتحام "، وهي المقابل للخزائن المؤمنة ضد السرقة. وهنا لا يكفي أن تكون الشبكة آمنة، بل الأهم من ذلك أن يقتنع العملاء بأنها آمنة. وبناء الثقة في تحقق عناصر الأمن السابق ذكرها ليست بالأمر السهل، على الأقل حتى هذه اللحظة، فما زال عامل التوجس والقلق من استخدام الشبكات في نقل المعلومات عاملاً مؤثرًا لدى العملاء من الأفراد والشركات التي تستخدمها. ويحتاج توافر الثقة إلى تثقيف العميل، وإتاحة الفرصة له للتجربة والتأكد من سلامة الإجراءات على مدى فترة زمنية مناسبة، حتى يتم بناء الثقة وترسيخها. وإلى أن تتوافر هذه الثقة، وإلى أن يكون توافرها مبنيًا على أسس قوية ومؤكدة، فإن مستقبل شبكات المعلومات سيظل موضع تساؤل. ولكنني لا أعتقد أن هذا الأمر سيطول.

الفصل الثاني
أساليب نقل المعلومات عبر الشبكات

بعد أن تناولنا في الفصل السابق موضوع " الأمن في عصر المعلومات "، وبينا أثر شبكات المعلومات على أمن المعلومات، كان لزاماً أن نتحدث عن أساليب نقل المعلومات عبر الشبكات، لأثر أسلوب النقل في أمن المعلومات، وهو موضوع هذا الفصل والذي سوف نعقبه بفصل آخر عن أنواع شبكات المعلومات.

نتحدث في هذا الفصل عن الأساليب المختلفة المستخدمة لنقل البيانات عبر شبكات المعلومات، فنوضح وسائط نقل المعلومات المختلفة من كابلات وأقمار اصطناعية وأشعة المايكروويف وموجات الراديو. ثم ننتقل بعد ذلك إلى شرح أهم البروتوكولات المستخدمة في نقل البيانات عبر الشبكات. وركزنا على أهم هذه البروتوكولات على الإطلاق، وهو بروتوكول(TCP/IP)، بما يشتمل عليه من بروتوكولات فرعية، مع التطرق إلى بعض البروتوكولات الأخرى ذات العلاقة التي تستخدم في نقل البيانات، مثل بروتوكولات (UDP) و (ARP) و (ICMP) وأنهينا هذا الفصل باستعراض بعض الخدمات التي تقدمها بروتوكولات (TCP/IP) مثل خدمات (Telnet) و (FTP) و (TFTP) و (DSN) و (SMTP) وبرامج(r) المساعدة.

٢-١ أساليب نقل المعلومات والمفاضلة بينها:

يتم نقل البيانات الرقمية عن طريق تحويلها إلى إشارات كهربية، فمثلاً يمكن تمثيل الرقم (١) بجهد كهربي قدره (+ ف فولت)، وتمثيل الرقم (٠) بجهد كهربي سالب (- ف فولت). وعملياً يحدث تشويه واضمحلال للإشارات الكهربية أثناء انتقالها من المصدر إلى وجهتها، بسبب ظروف الوسط الذي تنتقل خلاله المعلومات. وقد يصل الأمر إلى حد عدم استطاعة المستقبل التمييز بين الرقم (١) والرقم (٠)، مما يؤدي إلى تحريف الرسالة [Halsall ١٩٩٦] ويتوقف ذلك على ثلاثة عوامل رئيسية:

١- نوع الوسط المستخدم لنقل البيانات.

٢- معدل سرعة تدفق البيانات المنقولة.

٣- المسافة بين نقطة الإرسال ونقطة الاستقبال.

ولهذا السبب تم وضع مواصفات قياسية عديدة للحد من هذه المشكلة، بالإضافة إلى العديد من الإجراءات التي سنتعرض لها في هذا الكتاب مثل استخدام (Parity bit)، ومثل أجهزة التقوية التي توضع على مسافات لكي تحسن من مواصفات الإشارة الكهربية عبر خط النقل، بالإضافة إلى بعض إمكانيات التحقق من صحة الإرسال والاستقبال التي تتمتع بها بعض أجهزة " المودم ".

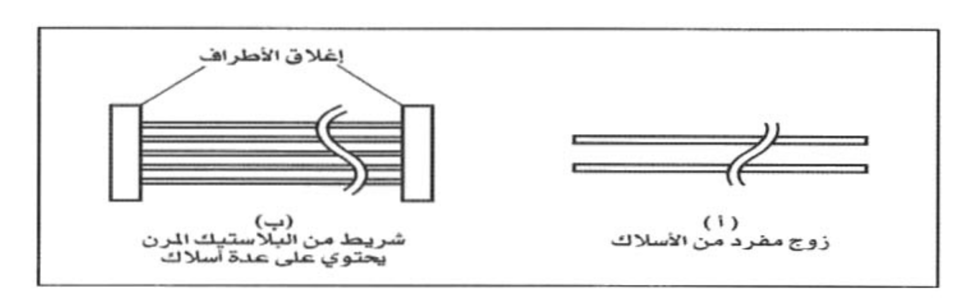
يتم نقل البيانات الرقمية خلال وسائط عديدة، ونوجز هذه الوسائط فيما يلي:

٢-١-١ الكابلات (Cables):

٢-١-١-١ الخطوط المزدوجة المفتوحة (Two-wire open lines):

يعتبر هذا النوع من أبسط وسائط نقل البيانات، ويستخدم سلكين يتم عزل كل منهما عن الآخر. وهذا النوع يناسب التوصيلات بين الأجهزة التي لا تتجاوز المسافة بينها ٥٠ مترًا، وسرعة النقل في هذا النوع متواضعة (أقل من ١٩,٢ kbps) أي أقل من ١٩ ألف بت في الثانية. وتمر الإشارة في السلك الأول، بينما يكون السلك الثاني موصولاً بالأرض (الجهد = صفر)، ويمثله الشكل (٢-١) أ ، ب.

شكل (٢-١)
الخطوط المزدوجة المفتوحة



وهذا النوع معرض للتداخل بين الإشارات التي تحملها الأسلاك(Crosstalk)، كما أنه ضعيف المناعة ضد الشوشرة (Noise)الناجمة عن الإشعاع الصادر من الأجهزة والمكونات المجاورة. وهذه هي الأسباب التي أدت إلى تحديد المسافة التي يصلح لها هذا النوع من وسائط نقل البيانات بما لا يزيد عن خمسين متراً.

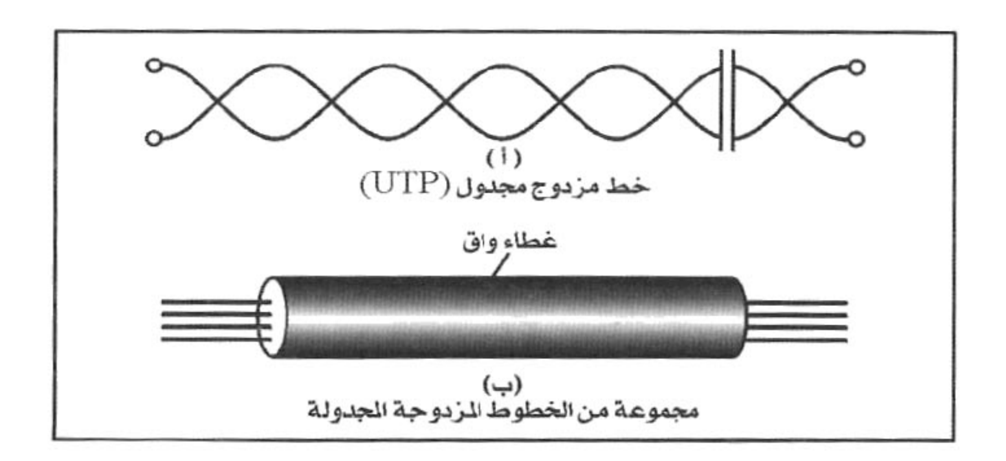
٢-١-١-٢ الخطوط المزدوجة المجدولة (Twisted-pair lines):

يمكن الحصول على مناعة أفضل ضد الشوشرة (Noise) باستخدام الخطوط المزدوجة المجدولة (Twisted-pair)إذ إن التفاف كل من السلكين حول بعضهما يقلل من تأثير الشوشرة، كما أن وجود أكثر من خط مزدوج مجدول ضمن الكابل الواحد يقلل من تأثير التداخل (Crosstalk)

ويصلح هذا النوع من وسائط النقل لنقل البيانات بسرعة في حدود (Mbps ١) أو مليون بت في الثانية عبر مسافات قصيرة (١٠٠ متر) أو بنقل سرعات أقل لمسافات أطول. وباستخدام دوائر استقبال متطورة يمكن زيادة سرعة النقل وزيادة مسافة النقل.

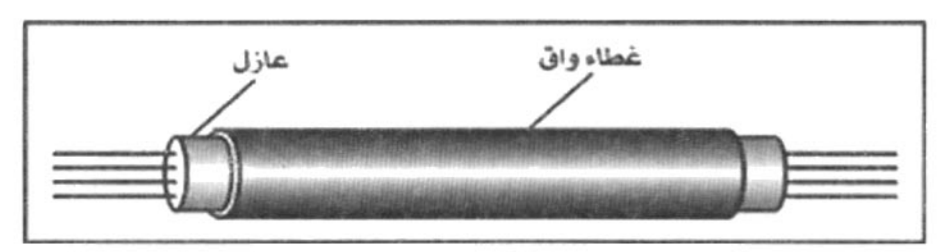
شكل (٢-٢)

الخطوط المزدوجة المجدولة (UTP)



ويطلق على هذا النوع اسم (UTP) أو (Unshielded Twisted Pair)، وهو مبين في شكل (٢-٢) أ ، ب. وينتشر استخدام هذا النوع في شبكات الهاتف وبعض شبكات نقل البيانات. وباستخدام الخطوط المزدوجة المجدولة المعزولة (STP) أو (Shielded Twisted Pair) يستعمل الغطاء الواقي والعازل لتقليل الشوشرة والتداخل كما يتضح من شكل (٢-٣).

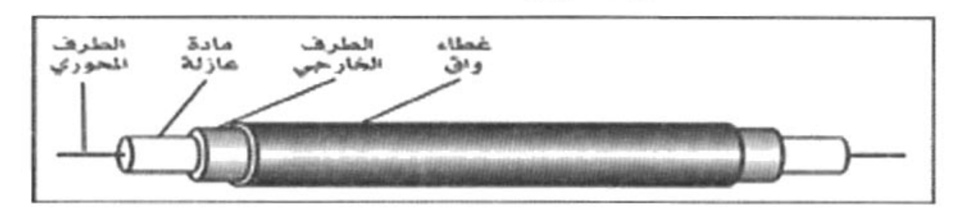
شكل (٢-٣)
الخطوط المزدوجة المجدولة المعزولة (STP)



٢-١-١-٢ الكابلات المحورية (Coaxial cables):

كان العيب الأساسي في استخدام الخطوط المزدوجة المجدولة (UTP) هو سعتها المحدودة وعدم قدرتها على نقل الترددات العالية بسبب ظاهرة سريان التيار في المحيط الخارجي للسلك(Skin effect)، حيث يسرى التيار في القشرة الخارجية فقط من السلك. ولذلك فبالنسبة للتطبيقات التي تحتاج إلى سرعات نقل بيانات أعلى من (١ Mbps) ظهرت الحاجة لاستخدام الكابلات المحورية (Coaxial cables) (شكل ٢-٤).

شكل (٢-٤)
كابل محوري (Coaxial Cable)



يقوم الطرف الخارجي بمهمة حماية (عزل) الطرف المحوري من الشوشرة والتداخلات الخارجية، كما يقلل من تأثير الإشعاع وظاهرة (Skin effect)، ولذلك يمكن استخدام هذا النوع من الكابلات حتى ترددات تصل إلى (١٠ Mbps) وعبر مسافات تصل إلى عدة مئات من الأمتار، أو إلى مسافات أطول بشرط تعديل الإشارة (Modulation).

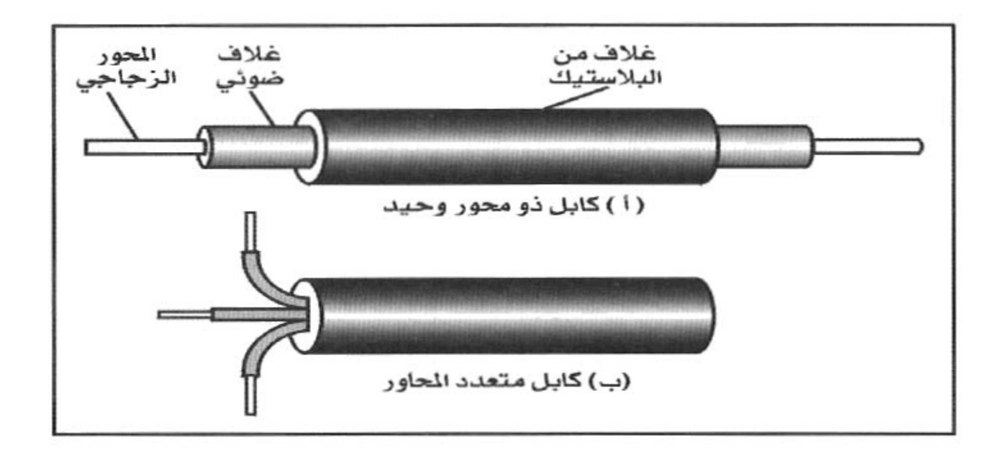
٢-١-١-٤ الألياف الضوئية (Optical fiber):

لم تحقق الكابلات المحورية طموح العلماء إلى سرعات نقل أعلى، مما حدا بهم إلى التوجه نحو الألياف الضوئية (Optical fiber) وهي تنقل البيانات في صورة شعاع متردد (Fluctuating beam) من الضوء في وسط من الألياف الزجاجية. فليست هناك إشارات كهربية ولا توجد أسلاك نحاسية. وتتميز الموجات الضوئية بسعة (Bandwidth) أكبر بكثير من الموجات الكهربية، مما يسمح بسرعات تصل - باستخدام وسائل الاستقبال المناسبة - إلى (٥٠٠ Mbps). وتتميز الموجات الضوئية كذلك بمناعتها ضد التداخل الكهرومغناطيسي وأنواع التداخل الأخرى (Crosstalk)، وهي مفيدة للغاية في نقل الإشارات منخفضة السرعة التي تكون معرضة لمستويات عالية من الشوشرة الكهربية مثل مصانع الحديد والصلب، أو حيث توجد مصادر للجهد الكهربي العالي، أو محولات الكهرباء. كما يستخدم هذا النوع من الكابلات بكثرة في الأحوال التي يكون فيها أمن المعلومات مهماً (وهو دائماً كذلك) حيث يصعب اختراق هذا النوع من الكابلات بهدف التنصت.

يتكون هذا النوع من الكابلات من ليف زجاجي واحد مخصص لحمل كل إشارة يتم نقلها، ويضم هذه الألياف التي يتكون منها الكابل غلاف حماية يتولى كذلك حماية الألياف الزجاجية من أي مصادر ضوئية خارجية قد تؤثر على الإشارة الضوئية المنقولة، ويبين شكل (٢-٥) مخططاً لهذا النوع من الكوابل.

شكل (٢-٥)

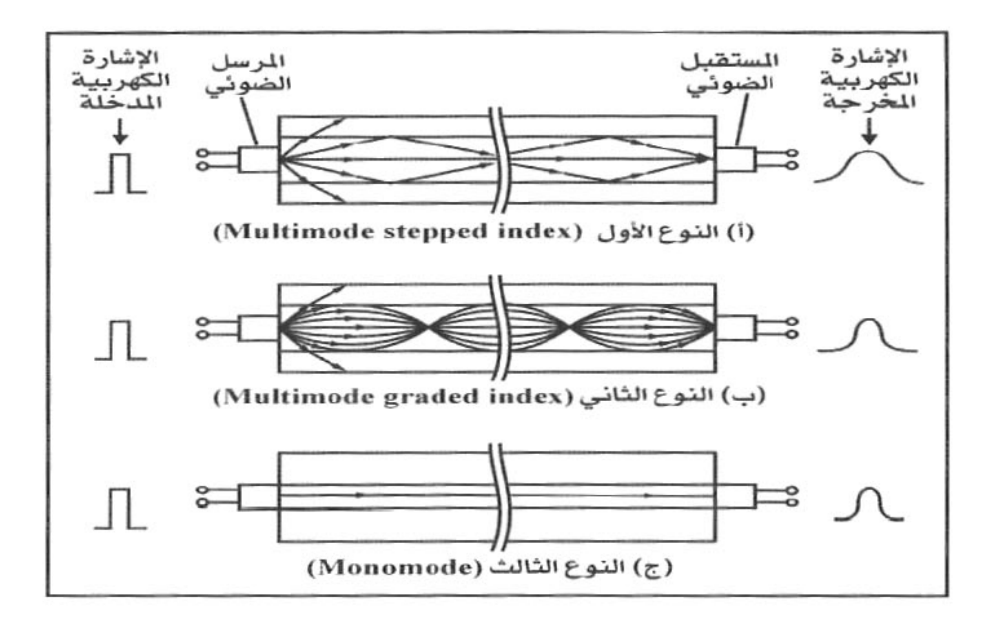
كابلات الألياف الضوئية (Optical Fibers)



يتم توليد الإشارة الضوئية عن طريق مرسل ضوئي (Optical transmitter)، والذي يقوم بتحويل الإشارة الكهربية العادية إلى إشارة ضوئية، فيما يقوم المستقبل الضوئي (Optical receiver) بالعملية العكسية في نهاية الخط. يتم هذا التحويل إما باستخدام قطب ثنائي باعث للضوء (LED) أى (Light-Emitting Diode) أو باستخدام قطب ليزر ثنائي (LD) أى (Laser Diode)، بينما يستخدم المستقبل في عملية إعادة التحويل قطب صورة ثنائي حساس للضوء (Light-sensitive photodiode) أو ترانزيستور الصورة (Photo transistor).

يتكون الليف الضوئي من جزأين: محور زجاجي، وغلاف ضوئي (Optical cladding) له معامل انكسار منخفض. ويسري الضوء خلال المحور الزجاجي بإحدى ثلاث طرق حسب نوع وسمك المادة المستخدمة. ويبين شكل (٢-٦) الطرق المختلفة لسريان الضوء وما ينتج عنها من إشارة.

شكل (٢-٦)
أساليب نقل الإشارة في كابل الألياف الضوئية



في النـوع الأول (Multimode stepped index) يكـون لكل من المحـور والغلاف معامل انكسـار مختلف، ولكنه ثـابت، بحيث إن الضـوء المنبعث من القطب الثنائي (Diode) الموجود في وحدة الإرسال، والذي ينبعث بزاوية أقل من الزاوية الحرجة، ينعكس على الغلاف الزجاجي ويسري خلال المحور عن طريق مجموعة من الانعكاسات الداخلية المتكررة كما يبين الشكل (٢-٦ أ). يستغرق الضوء مددًا زمنية متفاوتة ليسري خلال الكابل، وذلك وفقًا للزاوية التي يتم بها انبعاث شعاع الضوء من القطب الثنائي (Diode)، ويتسبب ذلك في أن يكون عرض النبضة في الإشارة المستقبلة أكبر من عرض النبضة الأصلي في الإشارة المرسلة. ويصاحب ذلك نقص في سرعة النقل القصوى يتوقف على درجة التشوه هذه. ولعل ذلك هو السبب وراء استخدام هذا النوع من الكابلات الضوئية في سرعات النقل المتواضعة، ومع الأقطاب الثنائية باعثة الضوء (LED) الرخيصة مقارنة بقطب الليزر الثنائي (Laser diode).

ويمكن معالجة هذا العيب باستخدام مادة للمحور الزجاجي يكون معامل انكسارها متغيرًا وليس ثابتًا كالنوع السابق، ويستخدم ذلك في الكابلات الزجاجية من نوع (Multimode graded index fiber) والتي تظهر في الشكل (٢-٦ ب). في هذا النوع يتم انكسار الضوء بشكل متزايد كلما ابتعدنا عن المحور، ويؤدي ذلك إلى تقليص عرض النبضة المخرجة مقارنة بالأسلوب الأول (Stepped index)، ويؤدي ذلك بالتالي إلى زيادة في الحد الأقصى لسرعة نقل الإشارة عبر الكابل.

يمكن الحصول على المزيد من التحسين في شكل النبضة المخرجة عن طريق خفض قطر المحور إلى ما يساوي طول الموجة (Mm ١٠-٣)، بحيث يسري كل الضوء المنبعث في خط واحد مستقيم تقريبًا كما يبين الشكل (٢-٦ ج). ويترتب على ذلك أن الإشارة المخرجة يكون عرض النبضة فيها قريبًا جدًا من النبضة المدخلة، مما يضمن عدم حدوث خطأ في تفسير البيانات المنقولة. هذا النوع (Monomode fiber)، والذي يستخدم عادة مع قطب الليزر الثنائي(LDs)، يمكن أن يعمل في سرعات تصل إلى (٣٠٠-٤٠٠ Mbps).

٢-١-٢ الأقمار الاصطناعية (Satellites):

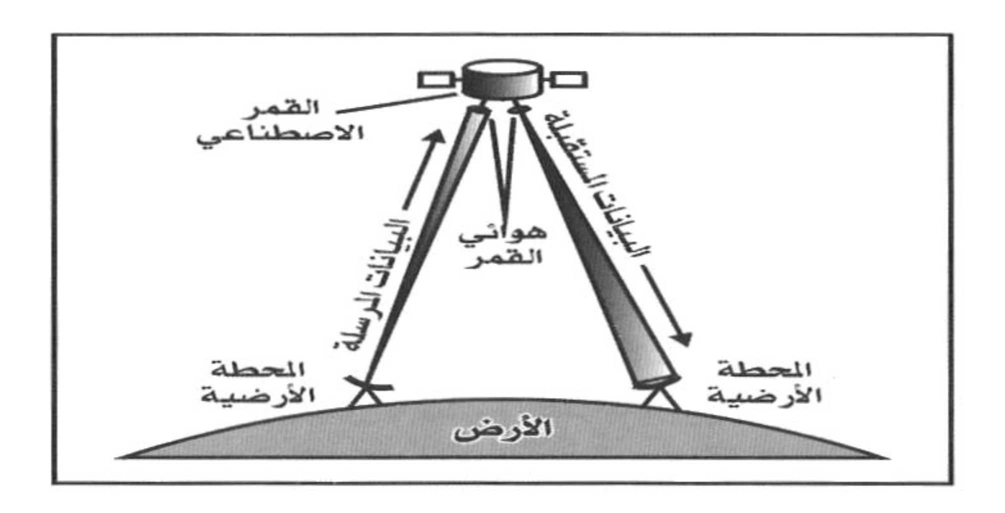
في كل وسائل النقل التي ذكرناها فيما سبق، استخدمنا وسائط مادية لكي تحمل المعلومات المطلوب نقلها. ولكن يمكن نقل البيانات باستخدام موجات الراديو (الموجات الكهرومغناطيسية) خلال الفضاء الخارجي كما يحدث في حالة النقل باستخدام الأقمار الاصطناعية، والتي بدأت بنقل المكالمات الهاتفية، ثم الصور التليفزيونية، والآن انتشر استخدامها في نقل البيانات الرقمية. ويتم ذلك باستخدام شعاع ميكروويف (Microwave beam) يحمل البيانات المطلوب نقلها بأسلوب التعديل (Modulation)، ويتم نقل هذا الشعاع من الأرض إلى القمر الاصطناعي. في القمر يتم استقبال هذا الشعاع ويعاد إرساله إلى وجهة محددة، وذلك باستخدام دائرة إلكترونية تسمى "دائرة النقل" (Transponder) والتي يوجد منها أعداد كبيرة في كل قمر اصطناعي. وكل

دائرة من هذه الدوائر تغطي مدى معين من الترددات (Band of frequencies).

تتميز قنوات القمر الاصطناعي بزيادة سعتها إلى حد كبير(٥٠٠ Mbps) ، وتستطيع توفير المئات من خطوط نقل البيانات (Data links) ذات السرعة العالية، باستخدام تقنية التوزيع (Multiplexing)، وتنقسم سعة القناة القمرية إلى قنوات فرعية يمكن تخصيص كل منها لخط نقل بيانات معين.

الأقمار الاصطناعية المخصصة للاتصالات يكون موضعها ثابتاً في السماء بالنسبة للأرض، أي يتم تحديد مدار القمر بحيث يجعله يدور حول الأرض مرة واحدة كل ٢٤ ساعة متزامناً مع دوران الأرض حول نفسها ولكن في الاتجاه المعاكس لدورانها. ويتم اختيار مدار القمر بحيث يكون له خط رؤية مباشر مع كل من محطة الإرسال ومحطة الاستقبال. وتختلف درجة تركيز شعاع الميكروويف المنبعث من القمر لنقل الإشارة. وتحدد درجة التركيز هذه كيفية وصول البيانات للمحطة الأرضية، فقد يكون الشعاع غير مركز (Coarse beam) ومن ثم يمكن التقاط الإشارة عبر مساحة جغرافية واسعة، أو يكون مركزًا بشدة (Finely focused beam) بحيث يمكن التقاطه في منطقة محدودة، وتستخدم أقمار التجسس أشعة غاية في التركيز حتى لا تلتقط الإشارة إلا في محطة الاستقبال المحددة فقط دون غيرها. ولكن هذا البث المركز يحتاج إلى إشارة قوية، ومن ثم إلى استخدام طاقة كبيرة بما يسمح باستخدام المستقبلات ذات الأقطار الصغيرة كالهوائيات (Antennas) وأطباق الاستقبال (Dishes).

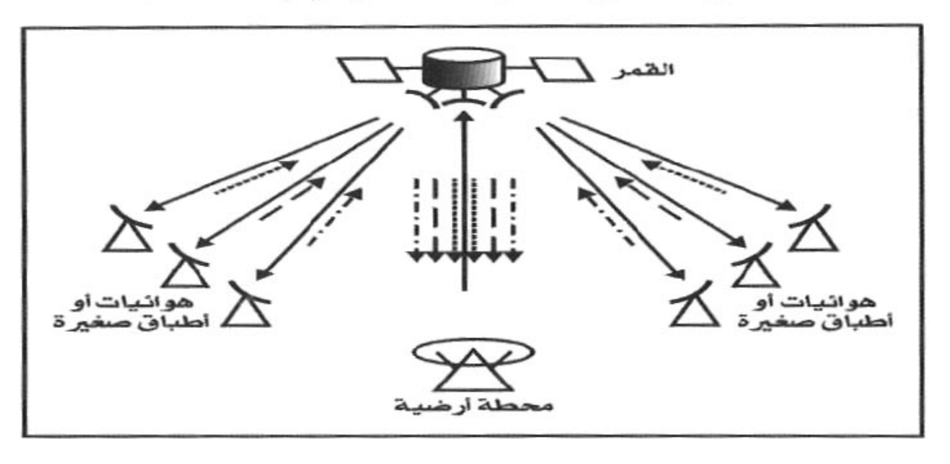
شكل (٢-٧)
نقل البيانات عبر الأقمار الاصطناعية (من نقطة لأخرى)



تستخدم الأقمار الاصطناعية على نطاق واسع في كافة التطبيقات التي تستخدم نقل البيانات، بدءًا من ربط شبكات الحاسبات في الدولة إلى توفير خطوط سريعة لربط شبكات الاتصال الهاتفي في أنحاء مختلفة من الدولة. يبين شكل (٢-٧) نظام النقل عبر الأقمار الاصطناعية من نقطة محددة إلى نقطة أخرى (Point to point). يبين الشكل عملية النقل وكأنها تتم في اتجاه واحد، ولكن الواقع أن كل خط يمكنه أن ينقل البيانات من القمر وإليه في نفس الوقت (Duplex transmission).

وقد ظهرات الاستخدامات العسكرية لهذه التقنية بوضوح في الحرب على العراق عام ٢٠٠٣م حيث تم نقل العديد من المعلومات من أرض المعركة مباشرة إلى القواعد الأمريكية في قطر إلى البنتاجون في الولايات المتحدة (داود ٢٠٠٤).

شكل (٢-٨)
نقل البيانات عبر الأقمار الاصطناعية (إلى عدة نقاط)



يمكن كذلك استخدام محطة أرضية للاستقبال من القمر ثم إعادة البث إلى هوائيات وأطباق أخرى في المنطقة المحيطة بالمحطة كما يبين الشكل رقم (٢-٨).

هذه الهوائيات أو الأطباق تسمى(VSAT) أي(Very Small Aperture Terminals). في هذه الحالة يرتبط كل هوائي أو طبق (VSAT) بجهاز حاسب آلي يتصل بجهاز حاسب مركزي كبير موجود في المحطة الأرضية كما يبين الشكل (٢-٨). وعادة يكون البث من المحطة الأرضية إلى الأطباق بتردد موحد، بينما يكون بث الهوائيات بترددات مختلفة. ومن أجل الاتصال بطبق معين (VSAT) تقوم المحطة الأرضية ببث الرسالة مع تحديد هوية الجهة المرسل إليها (VSAT) في مقدمة الرسالة (Header).

أما بالنسبة للتطبيقات التي تتطلب نقل البيانات من جهة إلى أخرى(VSAT to VSAT) فإن جميع الرسائل يتم إرسالها أولاً إلى المحطة الأرضية المركزية (من خلال القمر الاصطناعي) والتي تتولى بدورها إعادة بث الرسالة إلى الجهة المعنية. وفي الجيل الجديد من الأقمار الاصطناعية ذات الطاقة العالية يمكن إتمام التوجيه (Routing) من خلال القمر نفسه دون الحاجة إلى المرور من خلال المحطة الأرضية وهو ما نطلق عليه (Direct VSAT to VSAT).

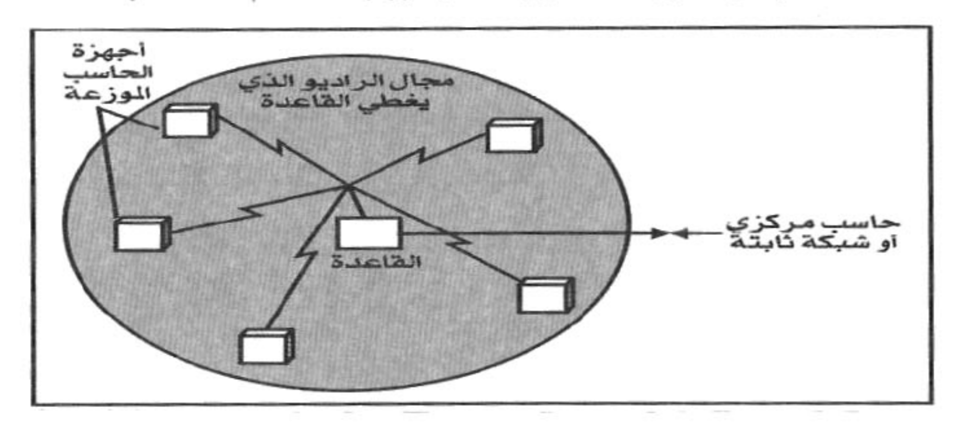
٢-١-٣ أشعة الميكروويف الأرضية (Terrestrial microwave):

تستخدم خطوط الاتصال باستخدام أشعة الميكروويف الأرضية (Terrestrial microwave) بكثرة لإتاحة خطوط الاتصال عندما يكون من غير العملي أو من المكلف جدًا إنشاء وسط مادي لنقل البيانات، عند الحاجة مثلاً إلى نقل البيانات عبر الأنهار أو الصحراء أو المستنقعات. ولكن عند انتقال شعاع الميكروويف المركز خلال جو الأرض قد يتأثر ببعض العوامل مثل وجود المباني العالية أو الظروف المناخية القاسية، ولكن باستخدام القمر الاصطناعي فإن هذا الشعاع يسري خلال الفضاء، ولذلك فهو ليس عرضة لمثل هذه العوامل. ولكن بصفة عامة فإن نقل البيانات باستخدام خطوط الميكروويف الأرضية (بفرض وجود خط رؤية مفتوح دون عوائق بين طبق الإرسال وطبق الاستقبال) يمكن أن يتم بكفاءة في حدود مسافة ٥٠ كيلو مترًا.

٢-١-٤ موجات الراديو (Radio waves):

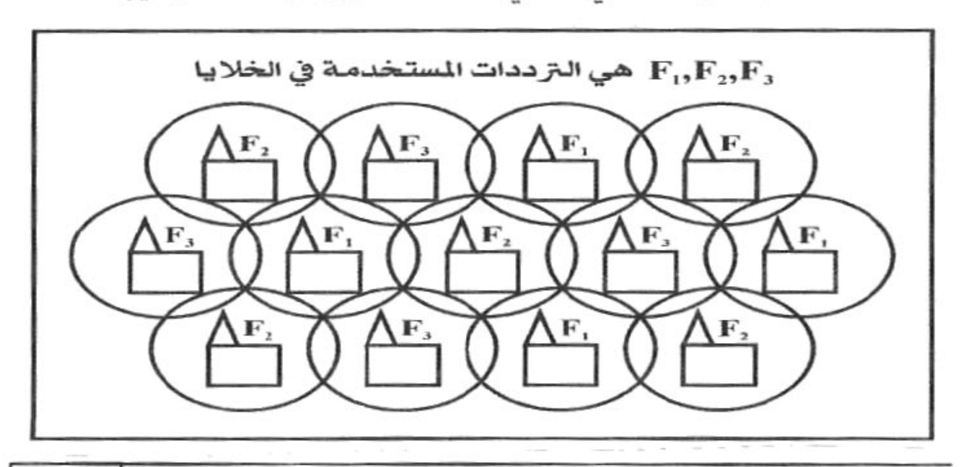
تستخدم موجات الراديو ذات التردد المنخفض كبديل عن الكابلات والأسلاك عبر المسافات القصيرة، وذلك باستخدام وحدات إرسال واستقبال أرضية. فقد تستخدم مثلاً من أجل توصيل عدد كبير من أجهزة الحاسبات الموزعة خلال مناطق مختلفة من الدولة بهدف جمع البيانات، أو قد تستخدم من أجل توصيل عدد من الأجهزة المستخدمة في منافذ الجوازات البرية والبحرية والجوية بالدولة، بحيث يتم تجميع البيانات المدخلة من هذه الأجهزة في حاسب مركزي ليتم تسجيلها (Logging) أو مراقبتها. في هذه الحالة يكون من المكلف كثيرًا مد شبكة كابلات، ولذلك تستخدم موجات الراديو لتشكل وسطًا لاسلكيًا بين نقطة محددة وعدد من أجهزة الحاسب الموزعة. ويوضع جهاز إرسال (Radio transmitter) يسمى " القاعدة " (Base station) في النقطة المركزية الثابتة كما بين الشكل رقم (٢-٩) ومن خلاله يتم الاتصال بين الحاسبات والنقطة المركزية.

الشكل (٢-٩)
نقل الإشارات بواسطة موجات الراديو باستخدام قاعدة ثابتة



ويمكن استخدام العديد من القواعد (Base stations) في التطبيقات التي تتطلب تغطية مساحات أوسع، أو التي تحتاج إلى عدد كبير من الأجهزة الموزعة. يمثل الشكل (٢-١٠) استخدام عدة قواعد (أو خلايا) متداخلة النطاق لتغطية مساحات كبيرة. وحجم كل خلية من هذه الخلايا لا يكون ثابتاً، وإنما يختلف حسب عدد الأجهزة التي تغطيها، وحسب الطبيعة الجغرافية للمنطقة التي تغطيها.

شكل (٢-١٠)
عدد من القواعد التي تغطي مساحات كبيرة بأشعة الراديو



تعمل كل من هذه القواعد باستخدام مجموعة من الترددات تختلف عن جاراتها المتداخلة معها، وطالما أن مجال التغطية لكل قاعدة هو مجال محدود فمن الممكن إعادة استخدام هذه الترددات في مناطق أخرى من الشبكة. ويتم توصيل هذه القواعد جميعها بالحاسب المركزي أو الشبكة الثابتة كما أوضحنا في حالة القاعدة الواحدة. وسرعة البث باستخدام هذا الأسلوب هي (٣٠-٤٠ Kbps).

يمكن تعميم استخدام هذا الأسلوب داخل المباني لإتاحة الاتصال اللاسلكي بين الحاسبات في المكاتب المختلفة، وفي هذه الحالة يتم وضع " قاعدة " (Base station) أو أكثر في كل دور من أدوار المبنى، ومن ثم ربطهم بالحاسب المركزي أو الشبكة الثابتة، وبذلك تغطي كل "قاعدة" مجموعة أجهزة الحاسبات التي تقع في نطاق تغطيتها. ويتفادى ذلك الحاجة إلى إعادة تمديد الكابلات عند تركيب جهاز حاسب جديد أو نقل جهاز من مكانه. ولكن ذلك يتطلب تركيب وحدة راديو تتولى تحويل البيانات إلى إشارة راديو ثم إعادتها إلى الصورة الثنائية مرة أخرى. ومن الجدير بالذكر أن سرعة نقل البيانات بهذا الأسلوب هي أقل من سرعة النقل باستخدام الكابلات.

٢-٢ بروتوكولات نقل البيانات:

هناك بروتوكولات يتم اتباعها عند نقل البيانات عبر الشبكات أو عبر خطوط الاتصال، والهدف من هذه البروتوكولات أن يتفق المرسل والمستقبل على مجموعة من القواعد والاتفاقات حول كيفية الإرسال وكيفية الاستقبال لضمان صحة إرسال واستقبال الرسائل. وسوف نقصر الحديث هنا على أهم هذه البروتوكولات وأكثرها استخداماً على شبكة الإنترنت وهو بروتوكول التحكم في النقل/ بروتوكول الإنترنت (TCP/IP) أو (Transmission Control Protocol/ Internet Protocol). وعند حديثنا عن تصميم جدران الحماية (Firewalls) سوف نوضح أهمية تحديد أي من هذه البروتوكولات والخدمات سيتم السماح باستخدامه بين الشبكة المطلوب حمايتها وبين شبكة الإنترنت.

٢-٢-١ ما هو بروتوكول(TCP/IP)؟

هذا البروتوكول هو أهم بروتوكولات الشبكات المستخدمة على شبكة الإنترنت لنقل البيانات من مكان إلى آخر. وهو لا يقتصر على بروتوكول (TCP) وبروتوكول (IP) فقط، وإنما يضم مجموعة من البروتوكولات والبرامج المساعدة (Utilities)، منها بروتوكول (ARP) أو (Address Resolution Protocol)، وبروتوكول (UDP) أو (User Datagram Protocol) [Loshi١٩٩٧] ولكن الأهم من بين هذه البروتوكولات هو بروتوكول (TCP) وبروتوكول (IP)، وسنبدأ بالحديث عن بروتوكول الإنترنت (IP) أو (Internet Protocol).

٢-٢-٢ بروتوكول الإنترنت(IP):

هذا هو البروتوكول الأساسي في مجموعة البروتوكولات المسئولة عن نقل حزم الرسائل (Packets) من مكان إلى آخر، وهو يتميز بالخصائص التالية:

- كل حزمة من حزم الرسائل تعتبر وحدة منفصلة قائمة بذاتها، ويقوم هذا البروتوكول بفحص المعلومات الموجودة في مقدمة الحزمة، ويستخدمها في التعرف على وجهة الحزمة حتى تصل إلى مستقرها. وبروتوكول الإنترنت (IP) لا يعنيه أن تصل هذه الحزم إلى وجهتها مرتبة بنفس ترتيب إرسالها.
- ليس من مهام بروتوكول (IP) أن يتأكد من وصول الحزمة إلى وجهتها، كل ما عليه هو أن يرسل الحزمة في الاتجاه الصحيح ويفترض أنها إما أن تصل إلى وجهتها، أو أن هناك بروتوكولاً آخر سيكون هو المسئول عن تحديد ما إذا كانت حزمة الرسالة قد وصلت أم لا.
- بروتوكول (IP) لا يعنيه مسار الحزمة خلال شبكة الإنترنت. فقرارات توجيه الحزمة لتسلك مسارًا معينًا، أو إعادة توجيهها عبر مسارات أخرى هي من مهام بروتوكولات أخرى. وكثيرًا ما تسلك حزم نفس الرسالة سبلاً مختلفة خلال رحلتها عبر شبكة الإنترنت.

تحدثنا كثيرًا عما لا يفعله بروتوكول (IP) ولم نتحدث عما يفعله هذا البروتوكول! إنه يتسلم البيانات من الحاسب المرسل ويقسمها إلى حَزم (Packets)، يطلق عليها (Datagrams)، بأحجام يمكن نقلها عبر شبكة الإنترنت. في الطرف المستقبل يعيد بروتوكول (IP) ترتيب هذه الحزم ويتيحها للحاسب المستقبل. وعند إرسال هذه الحزم يسجل بروتوكول (IP) عنوان الحاسب المرسل (Source IP address) وعنوان الحاسب المستقبل (Destination IP address) في مقدمة الحزمة (عندما نقول IP address فنحن نعني العنوان الشبكي لإحدى الجهات المشاركة في الشبكة). ومن مهامه أيضًا أن يقوم بإجراء بعض حسابات التأكيد مثل " المجموع الاختباري " (Checksum) على المعلومات الموجودة في مقدمة الحزمة للتأكد من صحتها. ولكن من المهم أن نعرف أن بروتوكول (IP) لا يقوم بهذه الحسابات التأكيدية على محتويات الرسالة نفسها.

٢-٢-٣ بروتوكول التحكم في النقل(TCP):

هذا البروتوكول يستخدم بروتوكول الإنترنت(IP)، ويضمن تقديم خدمة التوصيل الموثوقة بين طرفي الاتصال؛ فعندما يقوم بروتوكول (IP) بإرسال الحزم يتولى بروتوكول (TCP) مهمة التأكد من أن هذه الحزم قد وصلت إلى وجهتها بالشكل الذي يسمح بإعادة ترتيبها لتطابق الرسالة المرسلة.

ومن جانبه يقوم بروتوكول (TCP) بإجراء الاختبارات (Checksums)على البيانات المرسلة والتي تتضمنها الحزم (وليس مقدمة الحزمة التي سبق وأن فحصها بروتوكول (IP).

يتولى بروتوكول (TCP) كذلك ضبط تدفق البيانات لتجنب حدوث اختناقات في حركة مرور الرسائل، ويستخدم البروتوكول أرقامًا مسلسلة في مقدمة حزم الرسائل (TCP header) مما يمكّن بروتوكول (IP) من إعادة ترتيب الحزم بالترتيب الصحيح عند وصولها إلى الطرف المستقبل.

٢-٢-٤ بروتوكولات أخرى ذات علاقة:

ذكرنا أن بروتوكول (TCP) وبروتوكول (IP) ليسا هما الوحيدان في مجموعة (TCP/IP) وأن هناك مجموعة من البروتوكولات يؤدي كل منها مهمة محددة وسنعرض فيما يلي لهذه البروتوكولات.

٢-٢-٤-١ بروتوكول حزم المستخدم (UDP):

يشابه بروتوكول "حزم المستخدم " (UDP) أو(U ser Datagram Protocol) بروتوكول (TCP) في أنه يستخدم بروتوكول (IP) لتحريك حزم الرسائل خلال الشبكة، ولكن هذا البروتوكول لا يعطي تأكيداً بالوصول مثلما يفعل بروتوكول (TCP)، ولذلك فهو يستخدم في حالة التطبيقات التي لا تتطلب تأكيداً بوصول الرسالة (مع ما يصاحب هذا التأكيد من أعباء إضافية) مثل خدمة أسماء النطاق (DNS) و (Domain Name Service) حيث يتم تبادل المعلومات مع الحاسبات الأخرى من خلال هذا البروتوكول (UDP).

٢-٢-٤-٢ بروتوكول ترجمة العناوين (ARP):

نستخدم دائماً عنواناً (IP) لتحديد وجهة الرسائل عبر شبكة الإنترنت؛ فعندما يتم إرسال حزمة من شبكة إلى شبكة أخرى يتم تمريرها إلى موجه (Router)الذي يفحص العنوان (IP address) والمعلومات الموجودة في جدول التوجيه (Routing table) الخاص بالموجه، ومن ثم يقوم بإرسال الحزمة إلى الشبكة المقصودة، فإذا لم تكن هذه الشبكة متصلة مباشرة بهذا الموجه فيقوم بإرسال الحزمة إلى موجه آخر ليتولى هذه المهمة. وعند وصول الحزمة يحتاج الموجه الذي تلقاها، أو البوابة (Gateway)التي تلقتها، إلى معرفة العنوان المادي (Hardware address) و (MAC address) للحاسب المقصود بالرسالة. ولكن لما كانت العناوين (IP addresses) تأخذ شكلاً تفريعياً يسهل فهمه بواسطة أجهزة التوجيه المختلفة على شبكة الإنترنت فهذا العنوان لا يصلح في المرحلة الأخيرة من الرحلة

حيث نحتاج إلى العنوان المادي لتحديد الجهاز المطلوب توصيل الرسالة إليه وهو عنوان (MAC) وهي اختصار (Media Access Control). وهنا تأتي مهمة بروتوكول " ترجمة العناوين " (ARP) أو (Address Resolution Protocol) الذي يستخدم للترجمة بين العنوان (IP address) والعنوان المادي (MAC address).

٢-٢-٤-٣ بروتوكول متابعة الرسائل (ICMP):

يستخدم هذا البروتوكول لمتابعة وصول الرسائل والإفادة عن أي خطأ في وصول هذه الرسائل إلى وجهتها، وهو يستخدم من جانب بروتوكول الإنترنت (IP). وهو بذلك يؤدي مهامًا في غاية الأهمية بالنسبة للموجهات (Routers) وباقي أجهزة الشبكات التي تتصل مع بعضها من خلال شبكة الإنترنت. وهذا البروتوكول بدوره يستخدم بروتوكول الإنترنت (IP) لإرسال المعلومات التي يحصل عليها عبر الشبكة.

بروتوكول " متابعة الرسائل " (ICMP) أو (Internet Control Message Protocol) يحدد ما إذا كان هناك اتصال فعلي بين أي نظامين على الشبكة، وهو يستطيع كذلك أن يخبر الطرف المرسل من خلال رسائله المتنوعة أن الطرف المستقبل لا يستطيع التجاوب مع سرعة الإرسال العالية التي يرسل بها حزم البيانات، ويظل يرسل هذه الرسائل حتى يقلل الطرف المرسل من سرعة إرساله إلى الحد الذي يستطيع الطرف المستقبل التجاوب معه.

كما تستفيد الموجهات (Routers) من هذا البروتوكول في إخطار موجه أخر عن وجود طريق أفضل لمرور الرسالة، فيعاد توجيه الرسالة إلى الطريق المناسب. وهناك كذلك رسالة " تجاوز المهلة المحددة لوصول الرسالة " والتي يستخدمها الموجه لإخطار المرسل بسبب عدم وصول رسالته.

٢-٢-٥ أهم الخدمات التي تقدمها بروتوكولات (TCP/IP):

تتضمن قائمة الخدمات التي تقدمها مجموعة البروتوكولات التي تتضمنها مجموعة (TCP/IP) الخدمات التالية:

- خدمة (Telnet): وتستخدم للسماح لأحد المستخدمين بالدخول عن بعد إلى نظام حاسب آخر وتنفيذ بعض البرامج أو الأوامر عليه.
- خدمة (FTP): تستخدم هذه الخدمة (File Transfer Protocol) لنقل الملفات من حاسب إلى آخر ومن شبكة إلى أخرى.
- خدمة(TFTP): هذه الخدمة (Trivial FTP) هي قريبة الشبه بخدمة (FTP) وتستخدم من جانب بعض أجهزة الشبكة لنسخ بعض الملفات أو البرامج من الشبكة إلى أحد الحاسبات، ولكن هذه الخدمة لا تحتاج إلى تعريف الشخص الذي يستخدمها، أي لا تحتاج إلى اسم أو كلمة مرور.
- خدمة أسماء النطاق (DNS): هذه الخدمة (Domain Name Service) مفيدة لجعل تحديد أسماء النطاقات يتم مركزيًا.
- خدمة نقل البريد (SMTP): هذه الخدمة(Simple Mail Transport Protocol) هي التي تستخدم عند إرسال أو استقبال البريد الإلكتروني.
- برامج (r) المساعدة: صممت جامعة " بيركلي " مجوعة من الخدمات أطلقت عليها اسم برامج (r) المساعدة أو (r utilities) لتسهيل بعض المهام كثيرة الاستخدام على الشبكة. وسميت بهذا الاسم لأنها تستخدم عن بعد(remote access)، ويبدأ كل من أوامرها بالحرف (r) فنجد منها (rlogin) للدخول على الحاسبات الأخرى، ونجد (rsh) لتنفيذ الأوامر على الحاسبات البعيدة، ونجد (rcp) لنقل الملفات بين النظم المختلفة، ونجد (rwho) لجمع المعلومات عن مستخدمي الشبكة، ونجد (Uptime) لعرض قائمة بأجهزة الحاسب على الشبكة وبعض المعلومات عنها [Ogletree ٢٠٠٠].

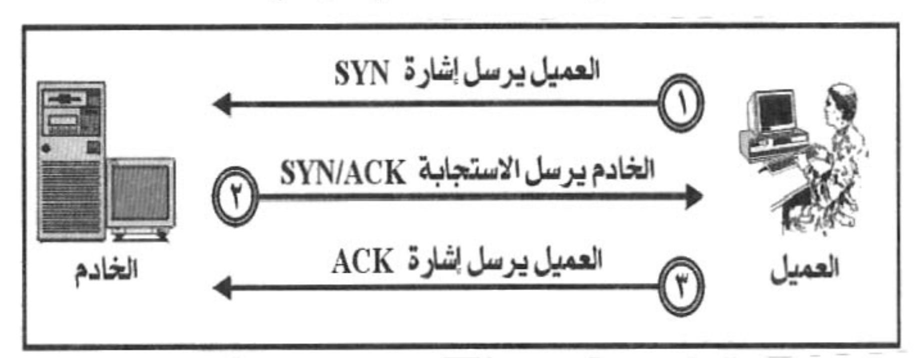
٢-٢-٦ عملية الاتصال الثلاثي المبدئي (TCP's ٣-way handshake):

تحدث عملية الاتصال الثلاثي المبدئي (TCP's ٣-way handshake) لإتمام الاتصال في البداية بين العميل (Client) والخادم (Server). وكانت هذه العملية إلى

حد قريب هي من أفضل المجالات التي يستغلها المهاجم لتنفيذ هجوم " عرقلة الخدمة " (Denial of Service)، إلى أن ظهرت أساليب أخرى أكثر فاعلية مثل (Smurf attack). نوضح فيما يلي كيف تتم عملية الاتصال الثلاثي المبدئي وكيف يتم استغلالها من جانب المهاجمين.

عند بدء الاتصال باستخدام بروتوكول TCP تحدث هذه العملية التي يوضحها شكل (٢-١١).

شكل (٢-١١)
عملية الاتصال الثلاثي المبدئي



(١) يقوم العميل بإرسال إشارة طلب الاتصال المبدئية (حزمة SYN) من منفذ معين على النظام إلى منفذ معين على نظام الخادم حيث يكون هذا المنفذ في وضع الترقب(LISTEN)، ويكون جهاز الخادم في وضع يسمح له باستقبال حزمة SYN أي وضع (SYN-RECV).

(٢) يقوم جهاز الخادم بالرد على إشارة العميل بإرسال حزمة (SYN/ACK) للعميل للدلالة على استقباله الإشارة السابقة واستعداده للاتصال.

(٣) إذا سار كل شيء على ما يرام يقوم جهاز العميل بإرسال حزمة (ACK) لجهاز الخادم ومن ثم تنتهي عملية التعارف ويصل الاتصال إلى حالة الاستقرار (ESTABLISHED).

برغم أن هذا النظام يعمل بشكل جيد معظم الوقت إلا أن هناك في هذا النظام بعض الثغرات التي يستغلها المهاجمون لتنفيذ هجوم " عرقلة الخدمة " (Denial of Service)، وتكمن المشكلة في أن معظم النظم تخصص عدداً محدوداً من الموارد عند بدء عملية الاتصال وبذلك فإن بعض النظم لا تتحمل مئات الاتصالات من خلال منفذ واحد (منفذ ٨٠ مثلاً) فتقبل هذه النظم عشرة أو عشرين اتصالاً قبل أن تمتلئ هذه الموارد بالكامل ويتوقف النظام عن استقبال الاتصالات، وهذا هو ما يعول عليه المهاجمون لتحقيق " عرقلة الخدمة" (DoS) [McClure ١٩٩٩] .

وسوف نتعرض بشكل مفصل لهذه الأنواع من الحزم والأوامر في الفصل التاسع من هذا الكتاب.

تبين لنا بوضوح في هذا الفصل أن الأسلوب المتبع لنقل المعلومات عبر الشبكات له تأثير كبير على أمن المعلومات، والشيء نفسه يمكن أن يُقال عن البروتوكولات المستخدمة في نقل المعلومات.



الفصل الثالث
شبكات المعلومات



بعد أن تحدثنا في الفصل الثاني عن أساليب نقل المعلومات عبر الشبكات، كان من الطبيعي في هذا الفصل أن نتحدث عن شبكات المعلومات، فنبين في البداية أهمية هذا النوع من الشبكات، ونتحدث عن بعض التقنيات المستخدمة مثل حاسب الشبكة (Network Computer) والحاسبات المتنقلة (Mobile Computers)، ومجموعات الحاسبات (Cluster Computers).

ثم نخصص قسمًا خاصًا لأنواع شبكات المعلومات، والتي نصنفها هنا وفقًا لنوع الاستخدام، فنتحدث عن شبكة الإنترنت وشبكة الإنترانت وشبكة الإكسترانت.

في القسم الذي يليه نتحدث عن بعض التقنيات المستخدمة في شبكات المعلومات مثل تقنية (DWDM)، والشبكة الضوئية المتزامنة (SONET) والمحولات الضوئية (Optical Switches)، وخط الألياف الضوئية حول الكرة الأرضية (FLAG)، والشبكات اللاسلكية، وبروتوكول التطبيقات اللاسلكية (WAP)، وشبكات الأقمار الاصطناعية (GEO) و (LEO) و (MEO).

في القسم الأخير من هذا الفصل نتحدث عن إحدى التقنيات الحديثة الواعدة وهي تقنية " خط المشترك الرقمي غير المتماثل " (ADSL).

٣-١ أهمية شبكات المعلومات:

تطور استخدام الحاسبات بشكل كبير في السنوات القليلة الماضية، وظهرت الحاجة إلى نقل البيانات بين هذه الحاسبات، ومن ثم ظهرت شبكات نقل المعلومات لأداء هذه المهمة، وتطورت بدورها تطورًا كبيرًا. وتكمن أهميتها في أنها تتولى ربط أجهزة الحاسبات في الإدارات المختلفة بالوزارات وفي المدارس والمعاهد ومراكز البحث العلمي. وتربط الشبكات أجهزة الحاسب في دور الصحف والمطابع والمستشفيات، وفي كل مكان يوجد به حاسب، فيندر الآن أن نجد حاسبًا ولا نجد شبكة.

٣-١-١ حاسب الشبكة (Network Computer):

تدعيمًا للاتجاه نحو الشبكات، ظهرت أنواع جديدة من الحاسبات تسمى "حاسب الشبكة " (NC) أو (Network Computer) يحتوي هذا الحاسب، الذي لا يمكن أن يعمل بدون شبكة، على المكونات الأساسية للحاسبات فقط دون وجود وحدات أخرى كوحدات التخزين (القرص الصلب) مثلاً. ويسمى هذا الحاسب (Thin Client)، ويعتمد في تنفيذ العمليات المطلوبة منه على وجود حاسب كبير بالشبكة التي يرتبط بها، بحيث يستطيع حاسب الشبكة استخدام طاقة التخزين العالية والبرامج الضخمة الموجودة على الحاسب الكبير [Halfhill١٩٩٧].

٣-١-٢ الحاسبات المتنقلة (Mobile Computers):

تطورت بعض أنواع الشبكات التي تربط الحاسبات المتنقلة (Mobile computers) بحيث يستطيع حامل الجهاز التنقل بحرية داخل المبني (أو خارجه) ويظل مع ذلك مرتبطًا بالشبكة. بل لقد تطورت بعض أنواع الحاسبات التي يمكن ارتداؤها (Wearable)، والتي أصبحت تستخدم الآن في قطاع الصناعة، حيث (يرتديها) الفنيون عند قيامهم بعمليات التصنيع والتجميع، و(يرتديها) الأطباء عند فحص المرضى والاتصال بالمستشفى لتوضيح حالة المريض قبل نقله إليه، ويستخدمها المراسلون الصحفيون في الاتصال بشبكات الأخبار التي يتبعونها لإرسال التقارير الصحفية وتلقي تعليمات الصحيفة [Ditlea ٢٠٠٠].

كل هذه التطبيقات ما كانت لترى النور دون وجود الشبكات.. شبكات المعلومات التي سهلت كل عمليات التواصل والاتصال بين الإنسان والآلة في مختلف المهن والصناعات والتطبيقات.

٣-١-٣ مجموعات الحاسبات (Cluster Computers):

تتطلب كثير من التطبيقات قدرات تفوق قدرة الحاسب المنفرد، وكان الأمر السائد

من قبل هو استخدام الحاسبات العملاقة (Super computers) لهذا الغرض، ولكن ارتفاع تكلفتها وعدم توافرها إلا في مراكز خاصة، وحجبها عن دول العالم الثالث وحاجتها إلى أنظمة تشغيل خاصة، ووحدات مساعدة خاصة، كل هذا جعلها غير عملية مما دفع إلى ظهور بديل أكثر مرونة وأقل تكلفة يسمى " مجموعات الحاسبات " (Cluster computers) [غنيمي ٢٠٠١].

ولم يكن ممكنًا ظهور هذا الاتجاه إلا بوجود شبكات الاتصالات السريعة بين الحاسبات لتبادل المعلومات، فنشأ نمط جديد من الحوسبة يسمى " حوسبة المجموعات " (Cluster computing). يشتمل هذا التجمع للحاسبات على مجموعة من الحاسبات التي تمثل " عقدًا " (Nodes) للشبكة، وتربط هذه الحاسبات جميعها شبكة سريعة لتبادل المعلومات. وكمثال على هذا الاتجاه توجد الآن في جامعة بيركلي بولاية كاليفورنيا الأمريكية " شبكة محطات العمل " والتي أطلق عليها اسم (OW) أو (Network Of Workstations)، والهدف منها هو إجراء البحوث في مجال نظم التصميم باستخدام الحاسب (Computer aided design)، ومجالات نمذجة الزلازل، ومحاكاة شبكات الحاسبات وغير ذلك. وكمثال آخر هناك مشروع " الألفية " (Millennium)الذي سيحتوي على عدد من الحاسبات يصل إلى ٢٩٠ حاسبًا. وتتجه كبريات شركات الحاسب إلى إعداد مواصفات قياسية عالمية ليتم اتباعها عند ربط أجهزة الحاسب.

٣-١-٤ نمو شبكة الإنترنت:

فرضت شبكة الإنترنت نفسها على العالم بكافة مجالاته واهتماماته، ففرضت نفسها حتى على رجل الشارع، وقد وصل عدد مستخدمي الشبكة في عام ١٩٩٩ إلى ١٨٠ مليون مستخدم، وفي عام ٢٠٠٠م إلى ٢٩٠ مليون مستخدم، ويتوقع أن يصل في عام ٢٠١٠م إلى ١١٠٠ مليون مستخدم [Nua ٢٠٠٣]، وهناك إحصاءات أخرى أكثر تحفظًا. وفي النهاية لا يوجد رقم محدد يمكن الثقة به في هذه الإحصاءات.

٣-٢ أنواع شبكات المعلومات:

هناك أكثر من أسلوب لتصنيف شبكات المعلومات، فقد نصنفها وفقًا للمساحة الجغرافية التي تغطيها الشبكة، فنجد الشبكات المحلية (LAN)، والشبكات المتوسطة (MAN)، والشبكات الكبيرة (WAN) [داود ٢٠٠٠ أ].

ويمكن تصنيفها حسب وسائط نقل المعلومات المستخدمة، فنجد " الشبكات الضوئية "(Optical fiber networks)، و" الشبكات اللاسلكية " التي تستخدم الأقمار الاصطناعية أو موجات الراديو، " والشبكات السلكية " التي تستخدم أنواع الكابلات المختلفة والتي أشرنا إليها بالتفصيل في الفصل الثاني " أساليب نقل المعلومات عبر الشبكات "، هذا بالطبع فضلاً عن التصنيف الثالث الذي يتم وفقًا لأسلوب الاستخدام، فنجد شبكة الإنترنت العالمية أو شبكة الشبكات، ونجد شبكة الإنترانت (Intranet) وهي الشبكة المحلية (LAN) التي تستخدم تقنيات الإنترنت داخل المؤسسة أو الوزارة، وشبكة إكسترانت (Extranet) عندما تتعامل المؤسسة مع العالم الخارجي والمستفيدين من خارجها. وأخيرًا هناك الشبكة الخاصة الافتراضية (VPN) أو(Virtual Private Network) وهي الشبكة التي تربط فروع الشركة أو الوزارة من خلال شبكة الإنترنت وتوفر الحماية والأمان للمعلومات المتبادلة عبر هذه الشبكة والتي سوف نخصص لها الفصل العاشر من هذا الكتاب.

وسنقدم فيما يلي بعض أنواع هذه الشبكات وفقًا للتصنيف الثالث:

٣-٢-١ شبكة الإنترنت:

عند حديثنا عن شبكة الإنترنت لا نود تكرار آلاف الصفحات التي كتبت عن هذه الشبكة، ولكننا سنقصر حديثنا عن الجيل الجديد لهذه الشبكة ومستقبلها.

في أكتوبر ١٩٩٦م اتفقت ٣٤ جامعة أمريكية على البدء في مشروع جديد للشبكات أسموه " إنترنت - ٢ " والهدف منه إنشاء بنية أساسية لشبكة جديدة تبلغ سرعة تداول

البيانات فيها ألف ضعف للسرعات التي كانت متاحة عند الاتفاق على إنشاء شبكة الإنترنت الحالية. هذا الاتجاه سيتيح تحقيق التكامل بين الوسائط المتعددة، ويتيح التفاعل المباشر مع نظم الحاسبات وقواعد المعلومات المنتشرة في هذه الجامعات، كما سوف يدعم هذا المشروع أسلوب " الحساب الموزع " (Distributed computing)، وسيرتفع بمؤتمرات الفيديو إلى آفاق أكثر رحابة تتيح دعم البحث العلمي التعاوني، كما ستدعم نظم التعليم عن بعد (Distance learning).

وبمرور الوقت ارتفع عدد الجامعات المشاركة في المشروع، ولم يعد قاصرًا على الولايات المتحدة فقط، بل شاركت دول أخرى حول العالم مثل كندا وألمانيا وسنغافورة والهند وإسرائيل وغيرها [غنيمي ٢٠٠١]. وتعتمد الشبكة الجديدة على أسلوب نقاط التجميع (Gigapops) أو (Gigabit-capacity point of presence) والتي تزيد سرعتها عن (Gbps ١) .

في الفترة نفسها أعلنت الحكومة الأمريكية عن " مبادرة الجيل الجديد من الإنترنت " التي انتهى العمل فيها في العام ٢٠٠٢م، لتشمل مجالات الرعاية الصحية أو " الطب عن بعد " (Telemedicine)، والتعليم عن بعد، والمكتبات الإلكترونية الرقمية، والبحث العلمي، والأمن القومي، والتطبيقات العسكرية، ومشروعات البيئة، وبرامج مواجهة الكوارث وإدارة الأزمات وغيرها. وهناك مشروع " المشاركة في البنية الأساسية للحوسبة المتقدمة "(PACI) أو (Partnerships for Advanced Computational Infrastructure) الذي يعتمد على ربط عدد كبير من الحواسب العملاقة وجعلها متاحة للاستخدام من خلال شبكة الإنترنت.

ولم تتخلف أوروبا عن الركب، فلدى الاتحاد الأوروبي مشروعه الخاص عن " الشبكة الأوروبية " (Trans-European Network) الذي يربط شبكات ١٤ دولة أوروبية.

وما دمنا نتحدث عن الجيل الجديد من شبكة الإنترنت فلابد أن نذكر مشروع (Teledesic) الذي يتضمن إطلاق ٢٨٨ قمرًا اصطناعيًا في مدار منخفض حول الأرض بتكلفة ٩ بلايين دولار.

الأرض بتكلفة ٩ بلايين دولار.

مما سبق يتضح أن هناك خطوات عملاقة ستجعل شبكة الإنترنت أكثر تطورًا وأكثر فاعلية، ولكنها في نفس الوقت ستكون أقل أمنًا كما سنرى في الفصلين القادمين.

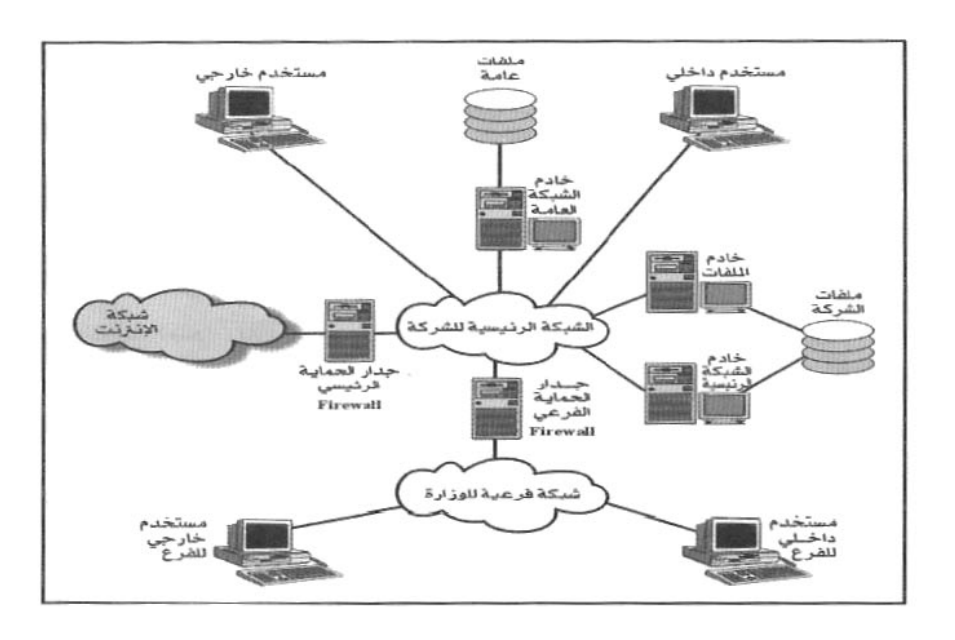
٣ـ٢ ـ٢ شبكة الإنترانت (Intranet):

هذا النوع من الشبكات هو ما تطور عن الشبكات المحلية (LAN) عندما اتجهت الشركات والوزارات إلى استخدام تقنيات الإنترنت في شبكاتها المحلية، فقامت باستخدام الصفحات الخاصة (Home pages)، واستخدمت تطبيقات (HTML) ، وبدأنا نرى الموظفين يدخلون على موقع الشركة لتقديم طلبات الإجازات أو لأداء مهامهم الوظيفية، مستخدمين برامج التصفح على الشبكة، كما أخذت هذه الجهات تستخدم نظم الأمن في الإنترنت مثل " جدران الحماية " (Firewalls)، من هنا نشأت "الإنترانت" (Intranet) وهي قد تحتوي على شبكات محلية (LAN)، وقد تتسع لتضم بعض الشبكات الكبيرة (WAN)، وبعض أجهزة تقديم الخدمة (Servers)، لكي تحفظ بيانات المؤسسة وقواعد معلوماتها. وتضم الشبكة كذلك أجهزة الموظفين (Clients)، وبعض برمجيات الإنترنت مثل برامج التصفح (Internet explorer) ومن أجل تأمين شبكة الإنترانت تستخدم بعض أساليب الحماية مثل " جدران الحماية "(Firewalls)، وأجهزة التفويض (Proxy) ، وأجهزة كشف الاقتحام (Intrusion Detectors). وتستخدم شبكة الإنترانت في المؤسسات كذلك لتبادل البريد الإلكتروني، وتنسيق الاجتماعات، باستخدام برامج مثل Outlook وغيرها من التقنيات التي كانت في الأصل مخصصة للاستخدام عبر شبكة الإنترنت.

أي أن شبكة الإنترانت يمكن تعريفها أنها الشبكة المحلية التي تستخدم تقنيات الإنترنت. وقد تنقسم شبكة الإنترانت إلى شبكات فرعية تضم فروع الشركة، ويبين

الشكل رقم (٣-١) مخططًا لشبكة الإنترانت.

شكل رقم (٣-١)
شبكة إنترانت بإحدى الشركات



٣-٢-٣ شبكة الإكسترانت (Extranet):

مع استخدام شبكة الإنترانت واستخدام تطبيقات البريد الإلكتروني الداخلي وتطبيقات جدولة الاجتماعات، ثم التوسع في ذلك بالخروج خارج حدود الشركة لكي تبني الشركة نظامها على أساس الاتصالات مع العالم الخارجي، وعندما تتخطى الشركة حدود المبنى لتشمل عملاءها الخارجيين والموردين والشركات المتعاونة معها، فإننا نجد أنفسنا أمام نوع جديد من الشبكات نطلق عليه اسم " إكسترانت " (Extranet). لكن التوسع في استخدام شبكة إكسترانت بواسطة الشركات قد يضر أكثر مما يفيد إذا لم تكن هناك عوامل الأمن والحماية اللازمة، فمع الخروج خارج حدود الشركة تزداد المخاطر وتزداد الحاجة إلى نظم الحماية. ومما يزيد الأمر

لتصبح آلية. وهنا يلزم الحذر في تطبيق شبكة إكسترانت وإلا تعرضت معلومات الشركة ومعلومات حلفائها للخطر [Erbschloe ٢٠٠١].

أتاحت شبكة الإكسترانت للشركات أن تتشارك في نظمها وشبكاتها المحلية مع جماعات أو شركات متباعدة جغرافيًا وبتكلفة منخفضة للغاية، كما أتاح هذا النوع من الشبكات للشركات التعامل مع موردي المواد الخام والتعامل مع الموزعين والعملاء بشكل متميز. ولكن ذلك لم يكن بغير ثمن؛ فقد كان الثمن بعض المخاطرة بأمن المعلومات.

وهناك مشروع " أيون " (Aion) الذي أعلنت عنه شركة (Computer Associates) واختارت له اسم " بلاتنيوم "(Platinum)، وهي أداة تعتمد على قواعد العمل (Business rules) وتستخدم لتطوير مكونات ذكية واستخدامها في كافة مجالات العمل بالمؤسسات، بما في ذلك تطبيقات إكسترانت وإنترانت. ويجمع هذا المشروع بين قواعد العمل (Business rules) والبرمجة الشيئية (Object-oriented programming) لإنشاء تطبيقات معرفية معقدة [Reynolds ٢٠٠٠]، ويعتبر هذا المشروع من التطبيقات المستقبلية المتقدمة التي تربط شبكات إكسترانت مع شبكات إنترانت.

٣-٢ التقنيات المستخدمة في شبكات المعلومات:

هناك العديد من التقنيات المادية (Hardware)، والبرمجية (Software)، والإجرائية (Procedures) التي تستخدم في شبكات المعلومات، بالإضافة إلى التقنيات المتمثلة في الهيكل العام (Structure) لبناء الشبكات. ويمكن الرجوع إلى كتاب " الحاسب وأمن المعلومات " من إصدار معهد الإدارة العامة [داود ٢٠٠٠ أ] لمعرفة هذه التقنيات واستخداماتها. ولذلك سنقصر المناقشة هنا على ما استجد من تقنيات في عالم الشبكات، وسنركز على التقنيات الحديثة في شبكات الألياف الضوئية.

ربما كانت كابلات الألياف الضوئية واحدة من أنجح وسائل نقل المعلومات وأكثرها

أمنًا وسرعة وفاعلية. وهي تتطور حاليًا بمعدل سريع لتأخذ مكانها على رأس قائمة وسائط نقل المعلومات، وتركز الأبحاث حاليًا على نقطتين: الأولى هي زيادة سرعات النقل عبر الألياف الضوئية، والثانية زيادة السعة لهذه الألياف لتنقل عددًا أكبر من الرسائل آنيًا ولتتسع لمدى أكبر من الترددات. وهناك تطبيقات بدأت في الظهور تحتاج بشدة إلى هذه السرعات والسعات العالية، منها " الحقيقة الافتراضية المباشرة " (Online Virtual Reality) والتي تحتاج إلى سعات تتراوح بين ١,٠٠٠ و ١٠,٠٠٠ تيرابت في الثانية. وهناك كذلك نظم "العرض الهولوجرافي ثلاثي الأبعاد" (٣-D Holography) وهي التي تسمح بتجسيد صورة مجسمة في الفراغ تحاكي الحقيقة إلى حد كبير. هذه التقنية تحتاج إلى سعات تفوق ذلك بكثير (من ٣٠,٠٠٠ إلى ٧٠,٠٠٠ تيرابت في الثانية).

نستعرض فيما يلي بعض التقنيات الحديثة المستخدمة في شبكات الألياف الضوئية:

٣-٢-١ تقنية "التجميع المبني على التقسيم الموجي المكثف"(DWDM):

تستخدم هذه التقنية لزيادة سعة الألياف الضوئية، وهي تسمى تقنية " التجميع المبني على التقسيم الموجي المكثف " (DWDM) أو (Dense Wavelength Division Multiple-xing) وهي تعتمد على نقل عدة إشارات على ليف واحد من الألياف الضوئية التي يتكون منها الكابل، وذلك باستخدام أطوال موجية مختلفة لهذه الإشارات. وتستخدم في هذه التقنية وحدات التجميع (Multiplexers)، ووحدات إعادة التوزيع (Demultiplexers)، وأجهزة تكبير الإشارات الضوئية، وغيرها من التقنيات المادية التي جعلت من تطوير الشبكات أمرًا ممكنًا. ومن خلال هذه التقنية أمكن زيادة السعة الكلية للكابل الضوئي بشكل كبير، وتتوقف هذه الزيادة على عدد أطوال الموجات، المستخدمة، وعلى سرعة نقل البيانات لكل من هذه الموجات ويوضح ذلك المثال التالي: لو كانت سرعة النقل للموجات المستخدمة هي ١٠ جيجابت في الثانية (١٠ Gbps) وتم استخدام ٤٠ موجة ذات طول مختلف فإن السعة الكلية ستكون:

السعة الكلية للكابل = سرعة النقل للموجة × عدد أطوال الموجات المستخدمة

السعة الكلية للكابل = سرعة النقل للموجة × عدد أطوال الموجات المستخدمة

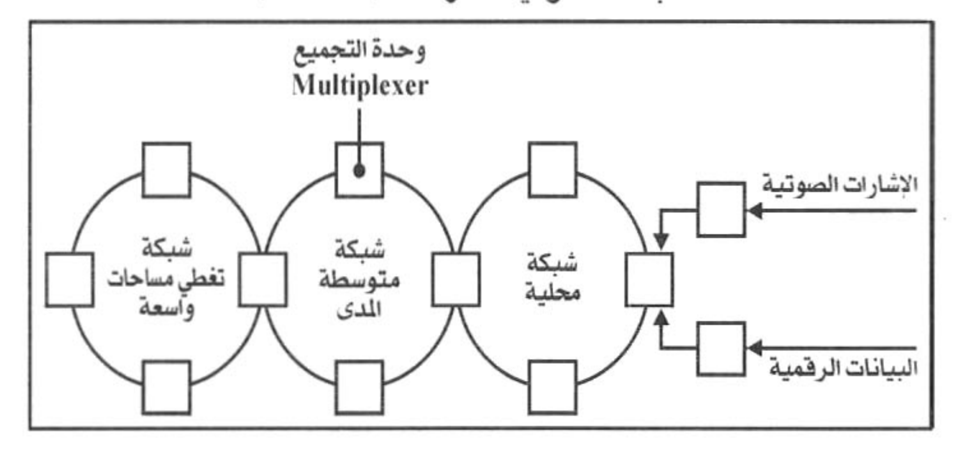
= ١٠ × ٤٠ = ٤٠٠ جيجابت في الثانية (Gbps ٤٠٠).

ويمكن الآن الوصول إلى ١٢٨ موجة، سرعة كل منها ١٠ جيجابت في الثانية، ومن ثم يمكن تجاوز سقف " التيرابت/ثانية " والوصول إلى سعة أكثر من (Tbps ١) [غنيمي ٢٠٠١].

٣-٣-٢ الشبكة الضوئية المتزامنة (SONET):

تمثل " الشبكة الضوئية المتزامنة " (SONET) أو-Synchronous Optical Net) (work أسلوبًا حديثًا لبناء هيكل (Structure) الشبكات الضوئية. في هذا الأسلوب يتم بناء الشبكة من وحدات نمطية متكررة عبارة عن حلقات مزدوجة من الألياف الضوئية، مصممة بحيث لا يتوقف عمل الشبكة عند حدوث أي قطع فيها، إذ يستمر سريان الإشارات المنقولة عبر النصف الثاني من الحلقة. وتستخدم هذه البنية في نقل الإشارات الصوتية والبيانات الرقمية، ويتوقع تعميم استخدامها لتكون أساسًا لنقل

شكل رقم (٣-٢)
الشبكة الضوئية المتزامنة (SONET)

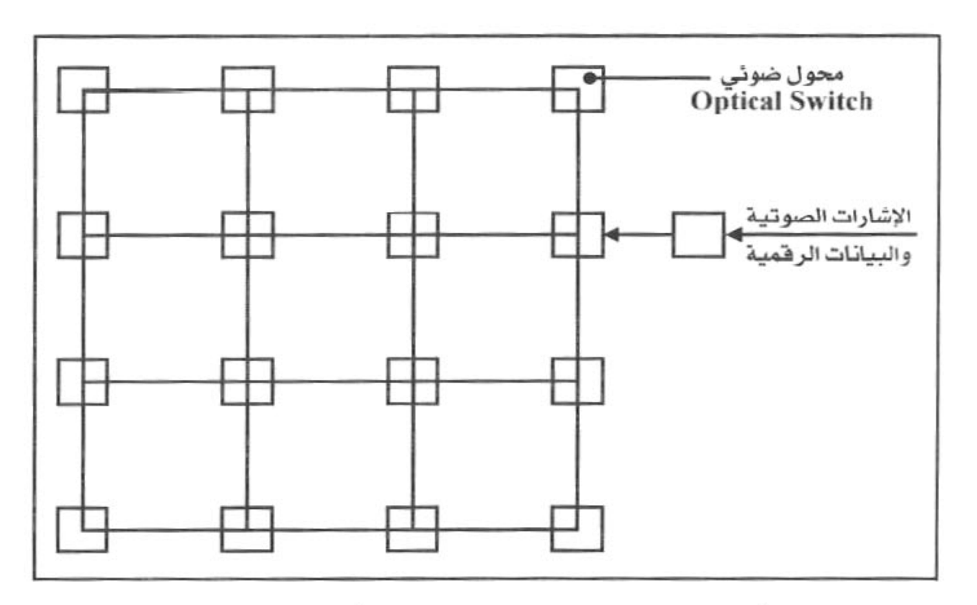


حزم البيانات (Packets)التي يتم نقلها عبر شبكة الإنترنت. ويبين الشكل رقم (٣-٢) كيفية عمل الشبكة الضوئية المتزامنة.

٣-٣-٣ المحولات الضوئية (Optical Switches):

للتغلب على مشكلة الازدحام في الشبكات وتعثر وصول الرسائل، يجب أن تكون هناك مسارات متعددة يتم من خلالها نقل المعلومات عبر الشبكة. ولذلك يتم استخدام " المحولات الضوئية " (Optical Switches) والتي يمكن استخدامها لإعادة توجيه حزم المعلومات من مسار إلى آخر كما يبين الشكل رقم (٣-٣).

شكل رقم (٣-٣)
استخدام المحولات الضوئية لتحويل مسار المعلومات



٣-٣-٤ خط الألياف الضوئية حول الكرة الأرضية (FLAG):

يمر الآن بالمملكة العربية السعودية خط الألياف الضوئية الذي يحيط بالكرة الأرضية ليشكل العمود الفقري للاتصالات السلكية في العالم. ويمر هذا الخط في البحار

استيعاب حركة نقل المعلومات في العالم. وتتفرع من هذا العمود الفقري شبكات فرعية كثيرة في كل الدول التي يمر بها لتغذي شبكات المعلومات الرئيسية في هذه الدول.

٣-٣-٥ الشبكات اللاسلكية:

تناولنا في الفصل السابق، في معرض الحديث عن وسائل نقل المعلومات، وسائل نقل البيانات دون كابلات أو أسلاك، وأطلقنا على هذا النوع من وسائل نقل المعلومات " الشبكات اللاسلكية "، وهي التي تستخدم موجات الراديو أو الأقمار الاصطناعية أو أشعة المايكروويف. وكانت وسائل النقل هذه هي التي مهدت الطريق لظهور الشبكات اللاسلكية، التي فتحت بدورها الباب واسعًا لعدد من التطبيقات الهامة مثل: التجارة الإلكترونية، والاتصالات الشخصية، والاستخبارات العسكرية، وإدارة الأزمات والكوارث، والتعامل في حالات الطوارئ، وتشغيل الأجهزة عن بعد، والاندماج مع شبكة الإنترنت. وتستخدم هذه الشبكات الحاسبات المحمولة والهواتف المحمولة، كما أنها تستخدم في بعض أجزائها الشبكات السلكية الثابتة عندما يكون ذلك أكثر جدوى.

وأصبح من السهل على مستخدمي الشبكات اللاسلكية الانتقال من مكان إلى آخر بأجهزتهم دون الحاجة إلى تمديدات لأسلاك أو كوابل. ويجب أن نعترف بأن هذا النوع من الشبكات، قد خلق قضايا أمنية بالغة التعقيد تتركز أساسًا في تعريف المستخدم والتحقق من شخصيته (Authentication) ويبلغ عدد مستخدمي نظم الاتصالات المحمولة في العالم حاليًا حوالي ٦٥٠ مليون مستخدم [GSMDATA ٢٠٠٣].

وهذا النوع من الشبكات يمكن أن يربط بين نقطتين لا تتجاوز المسافة بينهما عشرة أمتار، مثل نظام " السن الزرقاء "(Bluetooth)، أو أن تكون الشبكة عبارة عن شبكة محلية لاسلكية (LAN) تغطي موقع شركة كبيرة، أو تغطي جامعة تشتمل على عدة كليات متجاورة، أو قد تكون شبكة كبيرة (WAN) تغطي مساحة دولة كاملة أو مجموعة من الدول.

تستخدم الشبكات اللاسلكية " بروتوكول الإنترنت المتنقل "(Mobile Internet Protocol)، أو نظام " النقل اللاسلكي غير المتزامن "(Wireless ATM)، أو قد تستخدم الأقمار الاصطناعية في حالة الحاجة لتغطية مساحات كبيرة.

٣-٣-٦ بروتوكول التطبيقات اللاسلكية (WAP):

يمكن الآن للهواتف الجوالة أن تتصل بشبكة الإنترنت لاسلكيًا عن طريق " بروتوكول التطبيقات اللاسلكية " (WAP) أو (Wireless Application Protocol)، وقد بدأ بالفعل، في الجيل الجديد من الهواتف الجوالة، استخدام هذا البروتوكول في الدخول إلى شبكة الإنترنت واستقبال البريد الإلكتروني وتصفح " شبكة النسيج العالمية " (World Wide Web) [Wapforum ٢٠٠٤].

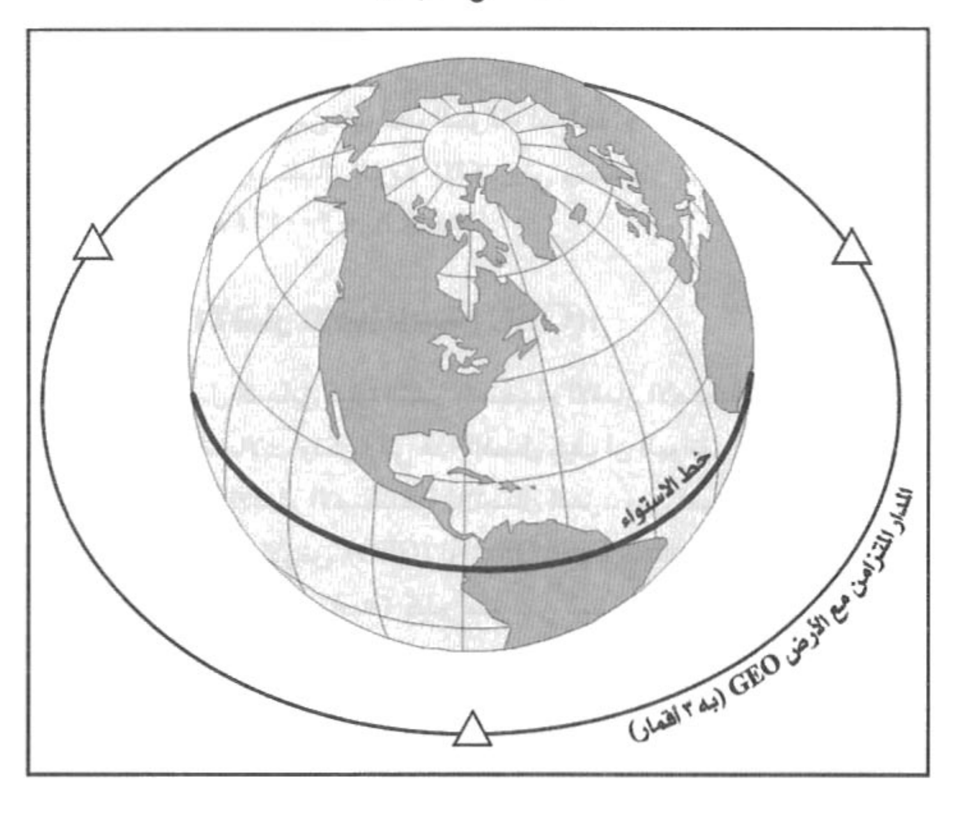
٣-٣-٧ شبكة الأقمار الاصطناعية (GEO):

ذكرنا في الفصل السابق كيف انتشر استخدام الأقمار الاصطناعية في عمليات نقل المعلومات ونظم الاتصالات، وذكرنا في هذا الفصل كيف أن الهواتف الجوالة قد استفادت من تقنيات النقل عبر الأقمار الاصطناعية للاتصال الحر. ومن أهم نظم أقمار الاتصالات نظام "المدار المتزامن مع الأرض" (GEO) أو(Geosynchronous Earth Orbit) حيث يبلغ ارتفاع مدار هذه الأقمار ٣٥,٨٠٠ كيلو متر عن سطح الأرض، وتحيط هذه الأقمار بالأرض في شكل حزام فوق خط الاستواء، وفي مقدور القمر الواحد أن يغطي ثلث مساحة الكرة الأرضية بسبب ارتفاع مداره بشكل مبالغ فيه، ومن ثم يمكن بثلاثة أقمار اصطناعية فقط تغطية اتصالات الكرة الأرضية بأكملها. ويبين شكل (٣-٤) هذه الشبكة من الأقمار المحيطة بالأرض.

اصطناعية فقط تغطية اتصالات الكرة الأرضية بأكملها. ويبين شكل (٣-٤) هذه الشبكة من الأقمار المحيطة بالأرض.

شكل رقم (٣-٤)

شبكة الأقمار الاصطناعية (GEO) ٣ أقمار على ارتفاع ٣٥,٨٠٠ كيلو متر عن سطح الأرض



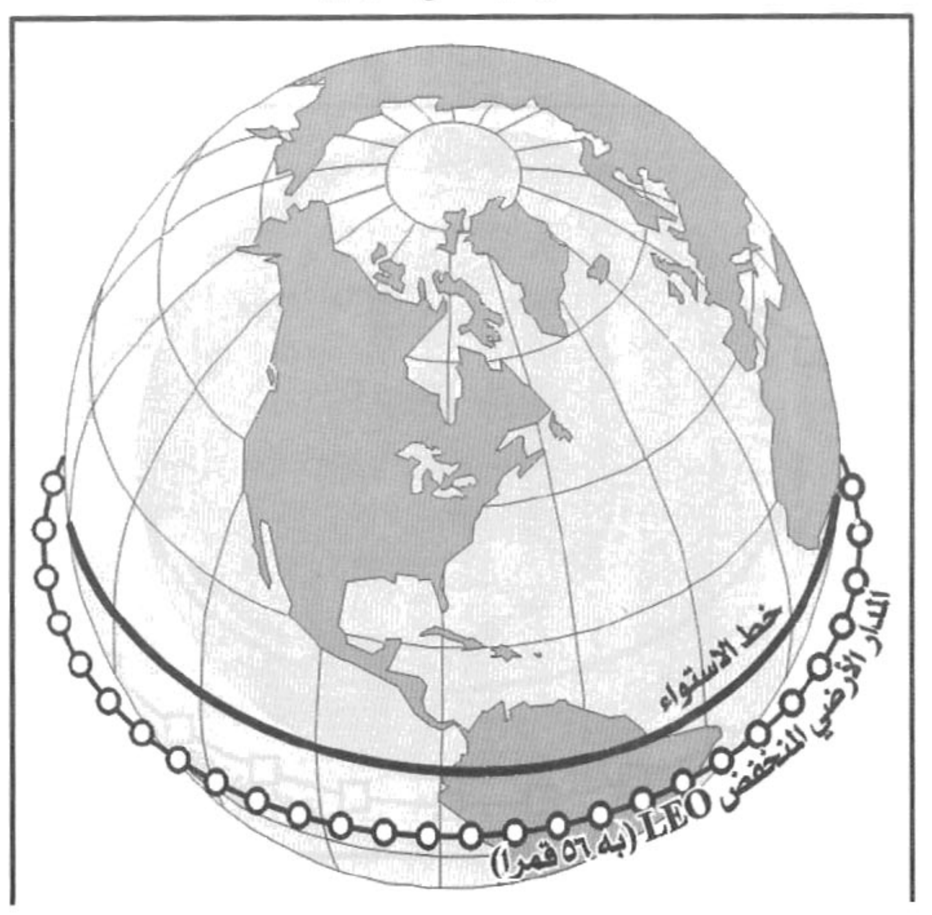
٣-٣-٨ شبكة الأقمار الاصطناعية (LEO):

هناك شبكة أخرى في طور التكوين تستخدم عددًا كبيرًا من الأقمار الاصطناعية، وذلك بسبب انخفاض مداراها، إذ يبلغ ارتفاع مدارها عن سطح الأرض ما بين ٥٠٠ إلى ١,٥٠٠ كيلو متر، وتسمى هذه الشبكة " المدار الأرضي المنخفض " (LEO) أوLow)

(Earth Orbit) وتستخدم عدداً من الأقمار يزيد عن خمسين قمراً. وبرغم زيادة عدد الأقمار إلا أن هذا النظام ربما كان أقل تكلفة من سابقه بسبب بساطة الأجهزة التي تحتويها هذه الأقمار لتغطيتها مساحات أقل من الكرة الأرضية ولعدم بعدها الكبير عن سطح الأرض. ويبين شكل (٣-٥) شبكة المدار الأرضي المنخفض.

شكل رقم (٣-٥)

شبكة الأقمار الاصطناعية (LEO) ٥٦ قمراً على ارتفاع ٥٠٠ إلى ١٥٠٠ كيلو متر عن سطح الأرض

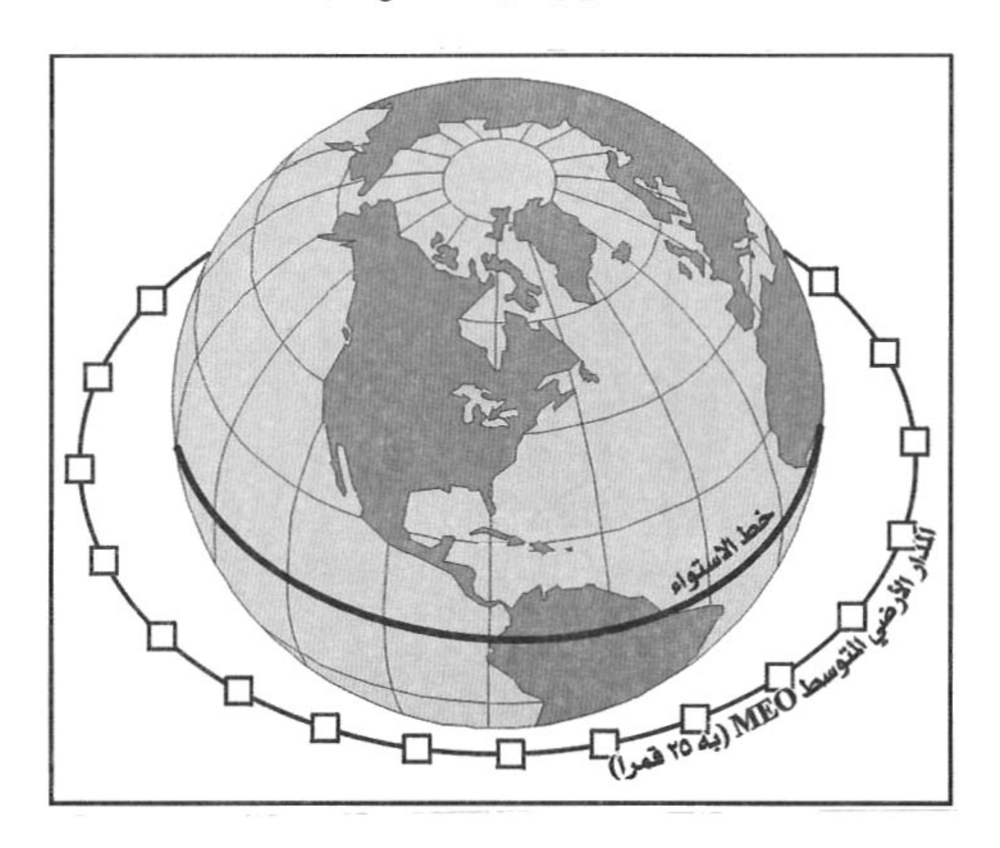


٣-٣-٩ شبكة الأقمار الاصطناعية (MEO):

بين الشبكتين السابقتين تقع شبكة " المدار الأرضي المتوسط " (MEO) أو (Medium Earth Orbit) والتي يبعد مدار أقمارها عن سطح الأرض ما بين ٥,٠٠٠ إلى ١٢,٠٠٠ كيلو متر.

ويبين شكل رقم (٣-٦) شبكة المدار الأرضي المتوسط (MEO).

شكل رقم (٣-٦)
شبكة الأقمار الاصطناعية (MEO) ٢٥ قمراً على ارتفاع ما بين ٥,٠٠٠ إلى ١٢,٠٠٠ كيلو متر عن سطح الأرض



٣ـ٣ـ١٠ شبكات الأقمار المستقبلية:

إحاطة الأرض بحزام من الأقمار الاصطناعية الخاصة بالاتصالات ما زال حلمًا يداعب خيال العلماء وأصحاب القرار في شركات الاتصالات، ولذلك فهناك عدة مشاريع كبيرة في هذا الاتجاه مثل نظام " جلوبال ستار " (Global Star) الذي يشتمل على ٤٨ قمرًا تدور حول الأرض على ارتفاع ١,٤٠٠ كيلو متر. ويذهب نظام (Teledisc) إلى أبعد من ذلك فيستعد أصحابه لإطلاق ٢٨٨ قمرًا على الارتفاع نفسه (١,٤٠٠ كيلو مترًا).

٣ـ٤ تقنية "خط المشترك الرقمي غير المتماثل" (ADSL):

تقنية " خط المشترك الرقمي غير المتماثل " (ADSL) أو(Asymmetric Digital Subscriber Line) هي من التقنيات الحديثة للاتصال بشبكة الإنترنت، ونتوقع أن يكون لها شأن في المستقبل، لذلك أفردنا لها قسمًا خاصًا في هذا الفصل.

٣ـ٤ـ١ إمكانيات تقنية (ADSL):

هذه التقنية، وهي من تقنيات " المودم "، تقوم بتحويل خطوط الهاتف الحالية من نوع الزوج المجدول (Twisted-pair) إلى خطوط اتصال للملتيميديا، ولتصبح بذلك وسيلة لنقل البيانات بسرعات عالية. ولهذا يطلق على هذه الوسيلة " وسيلة الوصول إلى طريق المعلومات السريع عن طريق خطوط الهاتف " أو (Twisted pair access to the information highway).

يمكن من خلال هذه التقنية نقل المعلومات في اتجاه واحد إلى المشترك بسرعة (٦ Mbps)، أو نقل المعلومات بسرعة (٨٣٢ Kbps) أو أكثر في كلا الاتجاهين أي من المشترك وإليه [ADSL ٢٠٠٣]. وهذه المعدلات العالية للسرعات ترفع الطاقة

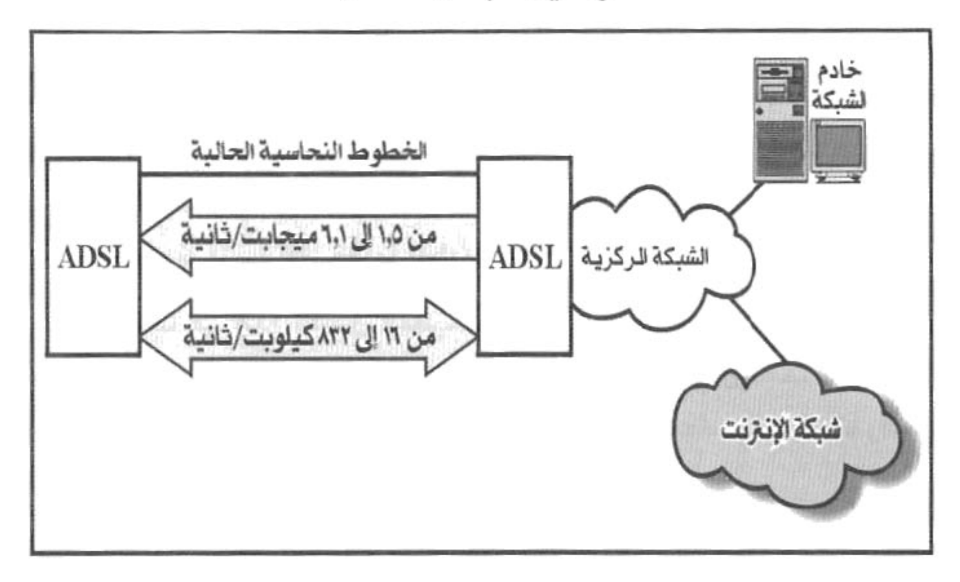
(٦ Mbps)، أو نقل المعلومات بسرعة (٨٣٢ Kbps) أو أكثر في كلا الاتجاهين أي من المشترك وإليه [ADSL ٢٠٠٣]. وهذه المعدلات العالية للسرعات ترفع الطاقة الحالية للخطوط خمسين ضعفًا على الأقل دون الحاجة إلى تمديد كابلات جديدة. تمكن تقنية(ADSL) من تحويل شبكة المعلومات العامة للدولة من شبكة مقصورة فقط على نقل الصوت والبيانات والرسوم ذات درجة الوضوح المنخفضة، إلى نظام قوي قادر على نقل تطبيقات الملتميديا وأفلام الفيديو ومؤتمرات الفيديو إلى منزل كل منا أو مكتبه.

ونتوقع أن تلعب تقنية (ADSL) دورًا ملموسًا خلال العقد المقبل، ونتوقع أن تساهم في دخول شركات الاتصالات ومقدمي خدمة الإنترنت إلى مجالات جديدة لنقل المعلومات التي تتضمن الفيديو والملتيميديا، بدلاً من الانتظار سنوات طويلة للاعتماد على شبكات النطاق العريض (Broadband networks) المنتظرة. ولكن نجاح هذه التقنية يتوقف على اشتراك عدد كبير من المستخدمين خلال السنوات القليلة القادمة، وفي هذه الحالة ستفتح شركات الاتصالات لنفسها أفاقًا جديدة ومجالات خدمة واسعة مثل نقل الأفلام وبرامج التليفزيون، وإتاحة الوصول إلى الأقراص (CD-ROMs)عن بعد، وربط الشبكات المحلية للشركات، وتنفيذ تطبيقات التجارة الإلكترونية وتطبيقات الحكومة الإلكترونية على نطاق واسع، وقد أتاحت تقنية (ADSL) العديد من التطبيقات

المتقدمة التي تتضمن إشارات الفيديو الرقمية المضغوطة. ويمثل الشكل رقم (٣-٧) كيفية توصيل شبكة (ADSL).

شكل رقم (٣-٧)

توصيل شبكة (ADSL)



٣-٤-٢ عمل شبكة (ADSL):

تربط دائرة (ADSL) جهازي المودم الخاصين بها على طرفي خط الهاتف العادي (Twisted-pair) لإنشاء ثلاث قنوات معلوماتية: قناة توصيل ذات سرعة عالية في اتجاه المشترك (Downstream)، وقناة ذات اتجاهين (Duplex channel) بسرعة متوسطة، بالإضافة إلى قناة شبكة الخدمات الرقمية المتكاملة (ISDN) أو (Integrated Services Digital Network) أو (POTS) وهي خدمة الهاتف العادية القديمة.

تتراوح سرعة النقل في القناة الأولى السريعة بين ١,٥ ميجابت/ثانية إلى ٦,١ ميجابت/ثانية، بينما تتراوح سرعة النقل في القناة الثانية (ذات الاتجاهين) بين ١٦ إلى

في حالة تعطل الاتصال من خلال (ADSL).

يمكن تقسيم كل من هذه القنوات إلى قنوات فرعية للحصول على عدة قنوات بسرعات أقل. ويوجد حاليًا خطوط اتصال (ADSL) تمزج بين النقل السريع في اتجاه المشترك (Downstream) بسرعة ٦ ميجابت/ثانية وخط النقل المزدوج (Duplex) بسرعة ٦٤٠ كيلوبت/ثانية.

ولما كان البث المباشر للفيديو الرقمي لا يستطيع استخدام نظم تصحيح الخطأ الحالية في شبكات المعلومات، لذا فإن أجهزة المودم الخاصة بتقنية (ADSL) تتضمن نظم تصحيح أخطاء خاصة تقلل بشكل هائل من الأخطاء التي تسببها الشوشرة الناجمة عن البيئة التي تنتقل خلالها المعلومات.

استعرضنا في هذا الفصل التقنيات الحديثة المستخدمة في إنشاء شبكات المعلومات، والخطط المستقبلية في هذا المجال الذي نظن أنه سيكون عصب التقنية في هذا القرن الجديد، وأن شبكات المعلومات سيكون لها الدور الحاسم في السلم والحرب على السواء.

الفصل الرابع
متطلبات الأمن في شبكات المعلومات

بعد أن استعرضنا في الفصل السابق أنواع شبكات المعلومات، نناقش في هذا الفصل المتطلبات الأمنية الواجب توافرها لتأمين شبكات المعلومات.

سنبدأ في القسم الأول من هذا الفصل بالحديث عن المخاطر التي تهدد هذه الشبكات وأنواعها، وأنواع المهاجمين الذين يهاجمون هذه الشبكات ودوافعهم لهذا الهجوم.

في القسم الثاني نبحث أثر انتهاك المعلومات على الشبكات، ثم نتطرق لتحديد احتياجات المؤسسات من البيئة الآمنة فنقدم تصورًا جديدًا للنموذج الأمني للمؤسسة (Enterprise Security Model)، وما تهتم به الإدارة العليا فيما يختص بالسياسة الأمنية للمؤسسة.

نختم الفصل بالحديث عن السياسة الأمنية للمؤسسات، وما يجب أن نجده في الوثيقة الأمنية، وما لا يجب أن نجده في هذه الوثيقة.

٤-١ المخاطر المحتملة:

يجب على مسئول أمن المعلومات أن يدرس المخاطر التي يحتمل أن تتعرض لها شبكة المعلومات. وبعد دراسة هذه المخاطر بعناية، يستطيع أن يصمم النظام الأمني المناسب للشبكة، كما يستطيع أن يتخذ الإجراءات المناسبة لمواجهة كل من هذه المخاطر. ولكن لابد لنا في البداية من تعريف المخاطرة.

٤-١-١ مفهوم المخاطرة:

عندما نتحدث عن المخاطرة فنحنِ نتحدث عن شيء غير مؤكد.. عن مجرد احتمال. فإذا لم يكن هناك شك فليست هناك مخاطرة، فالقفز من طائرة بدون مظلة لا يعتبر مخاطرة لأنه لا يوجد شك في النتيجة، ولا توجد احتمالات.. بل هي نتيجة واحدة. أما القفز باستخدام مظلة.. فهو مخاطرة محسوبة، فيها احتمالات نجاح كبيرة واحتمالات

فشل محدودة.

وعند ارتباط شركة بالإنترنت هناك شك في إقدام بعض المهاجمين على اختراق الشبكة الداخلية للمؤسسة، إذًا هناك مخاطرة. ولكن ما هي درجة هذا الشك؟ وما هي فرصة هؤلاء المهاجمين في النجاح في الاقتحام؟ .. هذا هو ما يحدد درجة المخاطرة .. وكلما زدنا احتياطات الحماية قلت المخاطرة، فكل ما نقوم به من إجراءات أمن لشبكات المعلومات هو لخفض درجة المخاطرة إلى أدنى حد ممكن. فركوب رائد الفضاء مكوك الفضاء الذي ينطلق به في الفضاء هو مخاطرة، ومن أجل تقليل درجة هذه المخاطرة وضعت " ناسا " نظامًا احتياطيًا كاملاً للنظام الاحتياطي نفسه، بحيث يعمل في حالة فشل النظام الاحتياطي، والنظام الاحتياطي يعمل آليًا في حالة فشل النظام الأصلي! هذا بالطبع من أجل خفض درجة المخاطرة إلى أدنى حد [Northcutt ١٩٩٩]. ولكن المخاطرة في مجال أمن شبكات المعلومات لا تصل إلى الصفر أبدًا.

ولذلك فمع أي مخاطرة يجب أن يكون هناك قرار مبدئي يتخذه مسئولو الأمن، وهو اختيار من بين ثلاثة بدائل: إما قبول المخاطرة كما هي، أو التدخل للتقليل من درجة المخاطرة، أو نقل المخاطرة إلى أطراف أخرى (مثل التأمين على الموارد).

٤-١-٢ أنواع المخاطر في شبكات المعلومات:

المخاطر عديدة في عالم الشبكات اليوم، ذلك العالم الذي يزيد فيه الاعتماد على انتقال المعلومة من مكان لآخر عبر الشبكة، ومن ثم لابد من معرفة أنواع هذه الأخطار، بل ومصادر هذه الأخطار ومرتكبيها. ومن المنطقي ألا نضع جميع المتعاملين مع المؤسسة موضع الشك وبنفس الدرجة، فلابد أن نولي الموظفين الذين يستخدمون الشبكة من الداخل ثقة أكبر من المتعاملين من الخارج، كما يجب أن نمنح مسئول أمن المعلومات ومسئول الشبكة قدرًا أكبر من الثقة. هذا القدر من الثقة قد يزيد من درجة المخاطرة، ولكنه يقلل إلى حد كبير من التكلفة الهائلة التي قد نتعرض لها إذا أردنا تأمين الشبكة من الجميع بلا استثناء وبلا ثقة.

دعنا الآن نحاول تصنيف أنواع المخاطر بصفة مبدئية إلى ثلاث مجموعات عامة [Kaeo ١٩٩٩]، على أن نتعرض بالتفصيل لأنوا ع المخاطر في الفصلين القادمين الخامس والسادس. هذه المجموعات الثلاث هي:

-الاستخدام غير المرخص به.

-انتحال الشخصية.

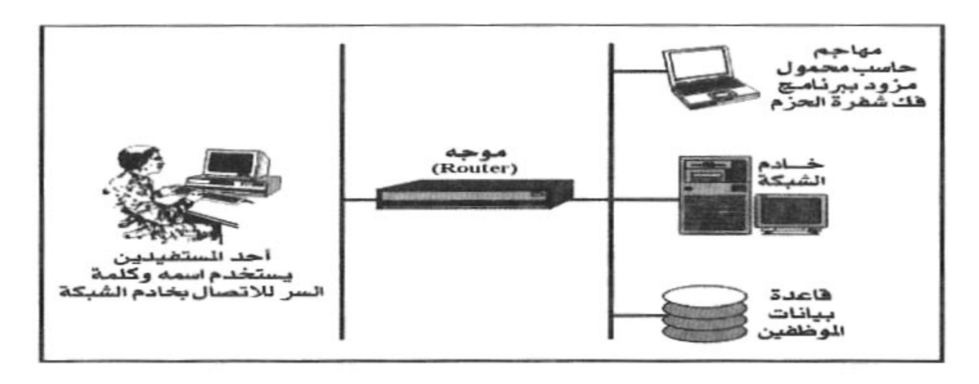
-عرقلة الخدمة.

٤-١-٢-١ الاستخدام غير المرخص به (Unauthorized access):

قد يتم دخول شخص ما أو جهة ما دون ترخيص إلى معلومات المؤسسة من خلال اعتراض هذه المعلومات خلال انتقالها عبر قناة توصيل غير آمنة، أو باستغلال ثغرة أمنية في أحد مكونات الشبكة. فيمكن مثلاً زرع وصلة في أحد الموزعات(Hubs) مركب بها حاسب لاقتناص حزم البيانات المارة والتنصت على المعلومات المسجلة بها، كما يمكن دخول المقتحم إلى أحد محولات " إيثرنت " ويتمكن من قراءة المعلومات المارة بشبكة " الإيثرنت "، باستخدام برنامج لفك شفرة حزم الرسائل، مثل برنامج (EtherPeek) أو برنامج (TCPDump).

شكل (٤-١)

الاستخدام غير المرخص به عن طريق برنامج فك شفرة الحزم



ويبين شكل (٤-١) دخول المقتحم عن طريق استخدام حاسب محمول واقتناص اسم أحد المستفيدين وكلمة السر الخاصة به عن طريق فك شفرة الحزمة المارة، وذلك باستخدام برنامج (EtherPeek). وبعد فك الشفرة ومعرفة الاسم وكلمة السر يستطيع المهاجم الدخول إلى خادم الشبكة أو إلى قاعدة بيانات الموظفين، كما يستطيع العبث بهذه المعلومات وتغييرها أو حذفها. وللأسف، فإن هناك برامج سهلة الاستخدام لفك شفرة الحزم متوفرة الآن وفي متناول الأفراد، حيث يمكن تركيبها على أي حاسب دفتري، والدخول إلى أي شبكة. هذه البرامج كان الهدف منها عند إنشائها تسهيل فحص مشاكل الشبكة (Troubleshooting)، ولكنها الآن يساء استخدامها.

وفي المقابل ظهرت في الأسواق بعض أجهزة التوزيع (Hubs) والتي (تتذكر) العناوين (MAC addresses) للأجهزة المتصلة بها، فإذا تم إقحام وصلة جديدة، أو جهاز جديد، بها استطاع مسئول الشبكة اكتشاف ذلك بسهولة.

٤-١-٢-٢ انتحال الشخصية (Impersonation):

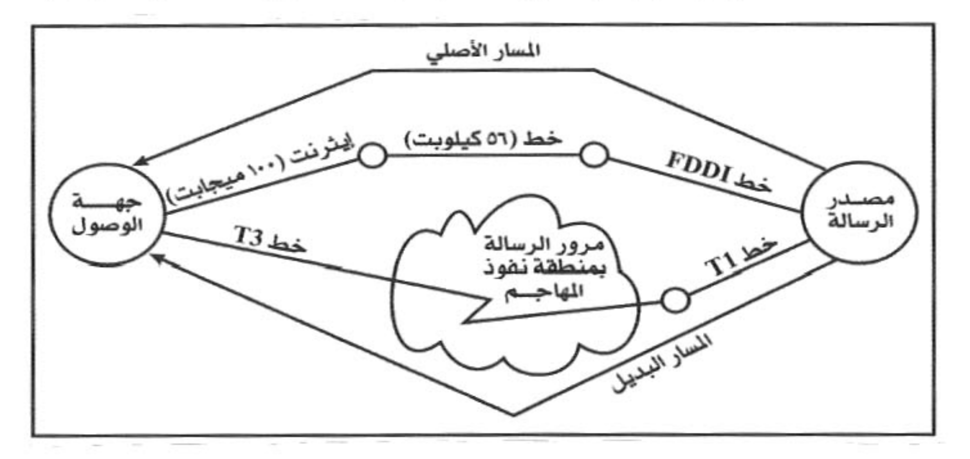
يمكن أن يحدث خطر انتحال الشخصية عن طريق قيام المهاجم بسرقة مفتاح التشفير السري، أو اقتناص الاسم وكلمة السر خلال مرورهما بالشبكة، أو بتسجيل بعض الرسائل المارة بالشبكة وإعادة إرسالها في وقت لاحق (Replay)، وهناك في الأسواق بعض البرامج الجاهزة التي تسهل تسجيل الرسائل وإعادة إرسالها.

قد يعمد المهاجم إلى انتحال شخصية شخص ما، وهذه الحالة يمكن مواجهتها بأساليب التحقق من الشخصية والتي سنتعرض لها بالتفصيل في الفصل القادم. هذه الأساليب تقلل من فرص نجاح محاولات انتحال الشخصية، كما يمكن لهذه الأساليب نفسها أن تكون دليلاً لا يملك معه مرسل الرسالة إنكار إرساله لها، وهذا أمر مهم في التحويلات المالية وبعض التطبيقات التي تتطلب إثبات قيام مرسل الرسالة بإرسالها. قد يعمد المهاجم في أحوال أخرى إلى انتحال شخصية " جهاز "، كأن يرسل رسالة يدعي صدورها من خادم الشبكة أو من خادم البريد الإلكتروني في الشبكة. فيمكن

مثلاً أن يقوم المهاجم بتزوير معلومات توجيه الرسالة (Routing information) بحيث يغير من مسار الرسائل الصادرة من مركز البنك الرئيسي مثلاً إلى أحد فروعه، بحيث تمر هذه الرسائل عن طريق آخر يمر بمنطقة نفوذ المهاجم. وفي المسار الجديد يمكن تزوير الرسائل أو تسجيلها أو منع مرورها كما يتبين من الشكل (٤-٢).

شكل (٤-٢)

انتحال الشخصية يتسبب في تحويل مسار الرسالة لتمر بمنطقة نفوذ المهاجم



٤-١-٢-٣ عرقلة الخدمة (Denial of Service):

المقصود بعرقلة الخدمة (DoS) أو (Denial of Service) هو حدوث انقطاع في خدمة الاتصال بالشبكة، أو بالخدمات التي تقدم للمستفيدين داخل الشبكة، وتتعدد الوسائل التي قد تسبب هذا الخطر. من هذه الوسائل إرسال حزم وهمية تملأ مساحات الذاكرة الوسيطة وتمنع الشبكة من مواصلة العمل (Buffer overflow) أو(SYN atta-ck) أو (SMURF attack). ومن هذه الوسائل أيضًا تخريب معلومات تجزئة الرسائل بحيث إذا حاول النظام المستقبل إعادة تركيبها عند الوصول، فإن هذه المحاولة تتسبب في تخريب النظام (Ping of Death) و (Teardrop attack). وسنتعرض في الفصول القادمة بالتفصيل لهذه الأنواع من وسائل عرقلة الخدمة وأساليب مواجهتها.

٤-١-٣ أنواع المهاجمين:

لكي نحدد الخطر الذي نتعامل معه لابد أن نعرف مصدره، ولذلك فمن المهم أن نتعرف على أنواع المهاجمين وعلى دوافعهم.

يشترك جميع المهاجمين في سمات معينة ومواصفات معينة، ربما كان أولها وأهمها هي رغبتهم في عدم الوقوع في قبضة العدالة. ولذلك فهم يعملون قدر جهدهم على إخفاء شخصياتهم، بل وإخفاء مكان وجودهم الجغرافي، أي يخفون الدولة والمدينة التي يمارسون منها نشاطهم الإجرامي.

سمة أخرى من السمات المشتركة لدى هؤلاء المهاجمين هي أنهم عندما ينجحون في اقتحام موقع ما فإنهم يعززون وجودهم فيه بفتح أبواب خلفية عديدة تمكنهم من العودة إليه مستقبلاً لو انكشف أمرهم، أو لو تغيرت مثلاً كلمة السر التي استخدموها في الدخول.

السمة الثالثة هي أنهم يميلون إلى العمل معًا، أي إلى التعاون وتبادل المعلومات مع غيرهم من المهاجمين، حتى أن لهم صفحات خاصة بهم على الإنترنت، وقوائم بريدية خاصة بهم، بل ومؤتمرات علمية خاصة بهم! أي أنه إذا نجح أحدهم في اختراق شبكة مؤسسة معينة فإن هذه الشبكة تعد في حكم المخترقة من جميع المهاجمين الآخرين. ليس هذا فقط، بل إن الموجات التالية من المهاجمين ستكون مهمتهم أسهل، ومن ثم فهم سوف يذهبون أبعد بكثير من (الرواد) الذين سبقوهم. ويمكن أن نصنف أنواع المهاجمين إلى الفئات التالية:

٤-١-٣-١ الباحثون عن التسلية:

هؤلاء هم بعض الأفراد الذين يعانون من الملل أو السأم ويبحثون عن التسلية، فيقتحمون الشبكات ظنًا منهم أنهم قد يجدون بعض البيانات المسلية، أو قد يتسلون باستخدام حاسبات المؤسسة التي يهاجمونها، أو لأنهم لا يجدون شيئًا آخر يشغلون به وقتهم.

بعض هؤلاء يخرجون إلى فضاء الإنترنت من باب الفضول وليس بهدف الإضرار العمد بالآخرين، وإن كانوا أحياناً يسببون الضرر عن جهل، أو خلال محاولتهم لإخفاء آثارهم بهدف تضليل مسئولي الأمن الذين قد يحاولون مطاردتهم. هذه الفئة تنجذب عادة إلى المواقع الشهيرة مثل وكالة " ناسا " لأبحاث الفضاء، ووكالة المخابرات المركزية الأمريكية، ووكالة " سي إن إن " للأنباء، وموقع " ياهو ".

في المملكة العربية السعودية اقتحم بعض المهاجمين السعوديين بعض مواقع الصحف السعودية الشهيرة واحتلوها لبضع ساعات، ويكاد يكون هذا حدثاً متكرراً لضعف إجراءات الحماية في هذه الصحف. وكنت على وشك أن أورد هنا بعض النماذج لهذه المواقع بعد اختراقها إلا أن بعض ما كان مكتوباً في الصفحة الرئيسية للموقع لا ترقى ألفاظه إلى المستوى الذي ألتزم به.

وخلال العام الماضي كانت لي حوارات عديدة مع مجموعة كبيرة ممن ينتمون إلى هذه الفئة من جنسيات عربية مختلفة، ووجدت لديهم نهماً كبيراً للمعرفة، وشغفاً بقبول التحديات، هذا الشغف إن تم توجيهه الوجهة الصحيحة لاستطعنا الاستفادة منهم بشكل كبير [داود ٢٠٠٣]. وقد تم تعيين اثنين من هؤلاء (كمستشارين) لبعض الوقت لإحدى الجهات الاقتصادية في مدينة الرياض.

٤-١-٣-٢ المخربون:

يعتبر المخربون أن مهمتهم الأساسية خلال تجوالهم في فضاء الإنترنت هي التخريب، وهم يفعلون ذلك إما من باب الحقد على الآخرين، أو لأن لهم مصلحة مادية في هذا العمل. وهؤلاء المخربون (أو العالم السفلي للإنترنت) يكونون ذوي خطر داهم بالنسبة للجهات التي يعتبرونها من (الأعداء). وهؤلاء الأعداء قد يكونون مثلاً صحيفة موالية للنادي الرياضي المنافس، أو جامعة رسب فيها عدد كبير من الطلاب، أو مقدم خدمة لا يعجب المخربين أداؤه، أو حتى شركة كبرى لها دعاية ضخمة، أو موقع له الآلاف من الزوار.

ومعظم المخربين يعمدون إلى التخريب المباشر والفوري وقصير الأمد، أي الذي يحدث أثره فورًا. وهذا النوع من التخريب تسهل، لحسن الحظ، مكافحته وإصلاح الأضرار الناتجة عنه. فهم قد لا يفعلون أكثر من أن يمسحوا البيانات من على جهاز الحاسب، أو يخربون التطبيقات العاملة على خادم الشبكة. أما إذا عمد بعضهم إلى تعديل البرامج أو تحريف البيانات أو تزوير المعاملات المالية، فهذا ينقلهم من هذه الفئة إلى فئة مجرمي الإنترنت. وهذه الفئة الأخيرة لها معاملة خاصة بصفتهم مجرمين، على العدالة أن تلاحقهم وعلى القضاء أن يقتص منهم. وللأسف يكاد يكون في حكم المستحيل إيقاف المخرب الذي لديه الدافع القوي والتصميم الكامل على اقتحام موقع ما.. فهو سيصل حتمًا إلى مبتغاه، طال الأجل أم قصر.

بعض أنواع الهجوم تجذب اهتمام بعض المهاجمين دون البعض الآخر، فعرقلة الخدمة مثلاً لا يجذب الباحثين عن التسلية، لأن هؤلاء الباحثين عن التسلية يهمهم أن يظل جهاز الضحية يعمل، وأن يظل متصلاً بشبكة الإنترنت حتى يتمكنوا من فعل ما يريدون.

٤-١-٢-٣ الساعون وراء تسجيل الأرقام القياسية:

نتساءل أحيانًا.. لماذا يقوم متسلقو الجبال بتسلق قمة " إفرست " أو غيرها من القمم الشاهقة؟ وماذا يجنون عندما يصلون إلى أعلى نقطة؟ إنهم فقط يريدون أن يقولوا للجميع أنهم قد وصلوا.. يريدون تسجيل أسمائهم في سجل من نجحوا في تحقيق شيء صعب.

الشيء نفسه تسعى وراءه هذه الفئة من المهاجمين، فئة الساعين وراء تسجيل الأرقام القياسية. فمرتبة المهاجم في العالم السفلي للإنترنت تتحدد تبعًا للنظم التي اقتحمها ومدى صعوبتها ومناعتها، وتبعًا لعدد العمليات التي قام بتنفيذها. ولذلك فهذه الفئة، شأنها شأن الفئتين السابقتين، يسعى أفرادها وراء المواقع الشهيرة و الحصينة التي يحدث اقتحامها دويًا هائلاً، وهذا هو مبتغاهم، فهذا هو ما يعطيهم

(نقطًا) أكثر في السباق نحو الصدارة. وهم في نفس الوقت قد يهاجمون مواقع بسيطة غير محمية بحثًا عن الكم وليس الكيف. وهم في معظم الأحيان لا يلحقون الدمار بالمواقع التي يقتحمونها ولكنهم يرفعون علمهم فوق الموقع الذي تم اقتحامه، وعلى أكثر تقدير يجمعون بعض المعلومات التي قد يقايضونها مع المهاجمين الآخرين بمعلومات أخرى عن مواقع أخرى، فالمعلومات السرية الثمينة مثل هذه أصبحت الآن عملة يتم بها البيع والشراء والمقايضة. وقد يلجأ بعض هؤلاء إلى استخدام الموقع المقتحم كنقطة وثوب يهاجمون منها مواقع أخرى.

أظهرت الأبحاث أن معظم أفراد هذه الفئة لا يقومون بأنفسهم بكتابة برامج الاقتحام أو كسر الشفرة لأنهم ليسوا مؤهلين علميًا أو فنيًا لذلك [Zwicky ٢٠٠٠]، وإنما يستخدمون برامج جاهزة ويتبعون تعليمات استخدامها، لذلك يطلق عليهم اسم (Script kiddies) وهم نتيجة لكثرة عددهم يسببون انتشار المعلومات عن المواقع التي ينجحون في اقتحامها بسرعة كبيرة في أوساط المهاجمين.

٤-١-٢-٤ الجواسيس:

هذه الفئة، فئة الجواسيس الاقتصاديين والسياسيين، تندرج تحت فئة المجرمين. فهم يسرقون معلومات سرعان ما تتحول إلى أموال، بعد بيعها أو بعد استخدامها، إذا كانت هذه المعلومات تتمثل في رقم بطاقة ائتمان مثلاً، أو تتمثل في رقم استخدام في إحدى شبكات الحاسب. وإذا عثروا بالمصادفة على سر من الأسرار فإنهم لا يتورعون عن عرضه للبيع.

لا توجد دولة في العالم اليوم ليس لديها جواسيسها المتخصصون في الحاسب الآلي.. إما للتجسس على الغير، أو للحماية من تجسس الآخرين. والتجسس لم يعد عسكريًا فقط، بل هو الآن بالدرجة الأولى تجسس اقتصادي وعلمي. وأصبح التجسس علمًا قائمًا بذاته، ولا يعتمد على مرونة وقدرات " جيمس بوند "، بل أصبحت أجهزة الحاسب وشبكاته هي ميدان القتال. وبالتالي أصبحت مكافحة التجسس أكثر صعوبة

من ذي قبل. وكشف الاقتحام، كما سنتحدث عنه في الفصل الثامن من هذا الكتاب، لا يمكن أن يكون فوريًا وناجحًا مع كل أنواع الاقتحام.

باختصار لا تستطيع الشركات والمؤسسات أن تضمن بقاء معلوماتها بعيدة عن أيدي جواسيس العصر الحديث. ولما كانت إجراءات الحماية الشاملة معقدة ومكلفة، فإن معظم الحكومات تعمد لوضع هذه الدفاعات القوية على عدد محدود من المواقع الحساسة فقط، وليس في كل مكان، وهذه الدفاعات سوف نتعرض لها في الفصول من السابع إلى العاشر. ولكن قبل استخدام هذه الوسائل الفنية التي سنتعرض لها مثل جدران الحماية وفاحصات الشبكة وأجهزة كشف الاقتحام والشبكات الخاصة الافتراضية، فلابد من اتخاذ بعض الإجراءات مثل استخدام الدروع الكهرومغناطيسية، أو عدم ربط الشبكة بالشبكات غير الآمنة، بالإضافة إلى الوسائل المادية لمنع غير المتخصصين من التواجد في الأماكن التي تسمح لهم بالدخول إلى أجهزة الحاسب المرتبطة بالشبكة. ومن أجل تجنب الاختراق بواسطة الجواسيس، على الجهات المعنية تأمين اتصال شبكتها بشبكة الإنترنت فهذا من أهم مصادر الخطر.

٤-١-٤ دوافع المهاجمين:

يساعد فهم دوافع المهاجمين على إعطاء صورة واضحة عن أكثر مناطق الشبكة عرضة للهجوم، وعن الإجراءات التي يحتمل أن يتخذها المهاجم. ولما كانت معظم أنواع الهجوم، كما رأينا في هذا الفصل، تأتي من شبكة الإنترنت، أي من خارج شبكة المؤسسة الداخلية، فإن أهم عناصر المنظومة الأمنية يصبح هو جدار الحماية الذي يفصل بين الشبكة الداخلية وبين شبكة الإنترنت. ويمكن تلخيص أكثر دوافع المهاجمين شيوعًا فيما يلي:

١- **الطمع:** قد يتم استئجار المهاجم بواسطة شخص آخر، أو مؤسسة أخرى، لاقتحام شبكة المؤسسة الداخلية وسرقة بعض المعلومات أو تعديلها، وذلك مقابل مبلغ من المال.

٢- **التسلية:** قد يكون المهاجم ممن يريدون التسلية ودفع الملل والضجر، ولذلك يقتحم هؤلاء بعض المواقع علهم يجدوا فيها ما يدفع عنهم الملل.

٣- **الشهرة:** قد يكون الدافع لاقتحام شبكة منيعة أو موقع شهير هو الحصول على الشهرة، وأن يضمن المهاجم لنفسه مكاناً وسط مجموعات المهاجمين.

٤- **الانتقام:** قد يكون المهاجم تعرض للظلم أو الاضطهاد أو الفصل التعسفي من العمل، ومن ثم يعمد من خلال الهجوم إلى تدمير بعض المعلومات الهامة الخاصة بالمؤسسة أو التسبب في عرقلة الخدمة واضطراب العمل.

٥- **الجهـــل:** ربما يكون المهاجم قد تعلم شيئاً ما عن استخدام الشبكات، وتعلم شيئاً ما عن الثغرات الموجودة بها، ومن ثم يكون نصف العلم (وهو أسوأ من الجهل) سبباً لارتكاب هذا المهاجم أفعالاً تسبب الضرر لشبكة المؤسسة، خاصة أنه سيكون من مهاجمي الداخل الذين تقل إجراءات الحماية ضدهم.

٦- **الإرهاب:** قد تتم بعض العمليات الإرهابية من خلال شبكة الإنترنت.

٧- **تنافس الغرماء:** قد يجد التنافس بين الغرماء من الشركات أو من الجماعات العرقية أو الدينية في شبكة الإنترنت متنفساً مناسباً.

٤-٢ أثر انتهاك المعلومات على الشبكات:

بعد أن تحدثنا في القسم الأول من هذا الفصل عن المخاطر المحتملة التي يلزم أن يواجهها مسئولو الأمن في الشبكات، وعن أنواع هذه المخاطر، وعن أنواع المهاجمين ودوافعهم، فمن المهم معرفة أثر نجاح هذه المخاطر على شبكات المعلومات. وهناك اتجاهان لتقييم أثر انتهاك المعلومات: التقييم الكمي، والتقييم الكيفي أو النوعي.

٤-٢-١ التقييم الكمي لأثر انتهاك المعلومات:

في نهاية الأمر يمكن ترجمة الخسارة المتوقعة إلى قيمة مالية.. حتى لو كانت

الخسارة معنوية، أو كانت فقداً للأرواح، أو كانت خسارة (لا تقدر بمال)، فإنها في النهاية يمكن ترجمتها إلى قيمة مالية. ينطبق ذلك على كل أنواع المخاطر التي ذكرناها. ولتقدير قيمة الخسارة المالية المتوقعة في حالة وقوع الكارثة التي يمثلها هذا الخطر، فإننا نتبع المعادلة التالية:

الخسارة المالية المتوقعة = قيمة المورد الذي خسرناه × درجة تعرض المورد

حيث درجة تعرض المورد هي عامل يتراوح بين الصفر إلى ١٠٠٪.

فلحساب التهديد الناجم عن انفجار قنبلة ذرية فوق مدينة صغيرة، إذا كان إجمالي الموارد بهذه المدينة هو ٤٠٠ مليون ريال فإن الخسارة المتوقعة = ٤٠٠ مليون ريال × ١٠٠٪ = ٤٠٠ مليون ريال، ذلك لأنه في حالة انفجار القنبلة الذرية فوق المدينة فإن جميع مواردها سيتم تدميرها.

والآن لندرس مثالاً آخر أقرب لواقع الحاسب الآلي، وهو دخول مهاجم إلى قاعدة بيانات المؤسسة التي تحتوي على معلومات هامة، ولنفرض أن هذا المهاجم قام بتشفير هذه المعلومات والاحتفاظ بمفتاح الشفرة رهينة في مقابل فدية يقدرها مثلاً بمبلغ مليون ريال. ما هو مقدار الخسارة في هذه الحالة؟ قد يقول قائل أن الخسارة هي مليون ريال. ولكن إذا كانت قيمة المعلومات تساوي مليوني ريال، مضافاً إليها الوقت اللازم لإعادة بنائها من الصفر، والخسارة الناجمة عن مدة توقف المؤسسة عن العمل، قد نصل إلى رقم يقارب الخمسة ملايين ريال. ولكن ماذا لو كان لدى الشركة " نسخة احتياطية " من هذه البيانات؟ الخسارة في هذه الحالة لن تتعدى تكلفة الوقت اللازم لاستعادة البيانات من النسخة الاحتياطية.

لذلك فإنني أدعو جميع الجهات التي تهتم بأمن معلوماتها للاهتمام بتوفير نسخة احتياطية من بياناتها باستمرار، لأن هذه النسخة ربما كانت هي طوق النجاة من الغرق في بحر تتلاطمه الأمواج.

٤-٢-٢ التقييم النوعي لأثر انتهاك المعلومات:

أحياناً لا نستطيع تقييم المعلومات بشكل مادي، مثل تحديد الأثر الناجم عن فقدان السمعة، أو الإساءة للمركز السياسي للدولة، أو الحرج الدبلوماسي. ويمكن الحصول على قائمة كاملة بهذه المجالات من موقع البحرية الأمريكية [Naval ٢٠٠٣]، ويبين الشكل (٤-٣) الصفحة الرئيسية للموقع.

شكل (٤-٣)
الصفحة الرئيسية لموقع البحرية الأمريكية



٤-٣ تحديد احتياجات المؤسسات من البيئة الآمنة:

تعتبر الخطوة الأولى لإعداد السياسة الأمنية للمؤسسة هي تحديد احتياجات هذه المؤسسة من البيئة الآمنة.

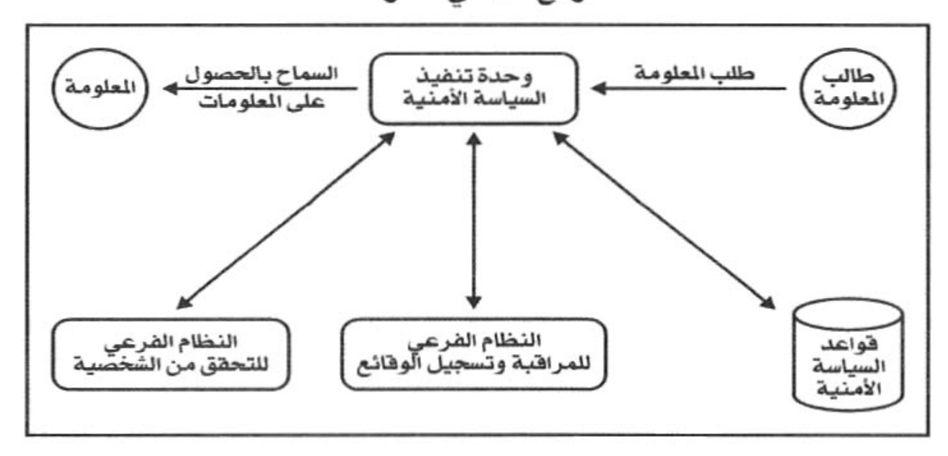
٤-٣-١ النموذج الأمني للمؤسسة (Enterprise Security Model):

لكي يمكن تحديد هذه الاحتياجات بشكل سليم نلجأ لبناء " النموذج الأمني للمؤسسة " (Enterprise Security Model) وربما كان أول من فكر في وضع نموذج أمني لنظم الحاسب الآلي هو " أندرسون " في عام ١٩٧٢، وخضع هذا النموذج لعدة تعديلات في الوحدات والمسميات حتى جاء " إسكاميلا " في عام ١٩٩٨ الذي طور من هذا النموذج بشكل كبير، وإن كان " إسكاميلا " قد مال إلى التعقيد بعض الشيء [Escamilla ١٩٩٨]. ونقدم في هذا الكتاب تطويرًا أكثر اقترابًا من الواقع، وبصورة تسمح بتحديد الموضع المناسب للأجهزة والأدوات الأمنية فضلاً عن المستفيدين والتطبيقات وقواعد البيانات وقواعد السياسة الأمنية في منظومة واحدة تسهل التصور العام للسياسة الأمنية وتسهل مراقبة تطبيق هذه السياسة.

فكرة هذا النموذج مبنية على أن هناك مجموعة من الوحدات أو الأفراد التي تطلب المعلومات ونطلق عليها اسم " طالب المعلومة "، وأنها تحتاج إلى هذه المعلومات من وحدات أخرى تحتفظ بهذه المعلومات أو تحتوي على هذه المعلومات ونطلق عليها اسم " المعلومة ". وعندما تنوي المؤسسة اقتناء أحد أدوات أمن المعلومات (سواء كان ذلك جهازًا أو برنامجًا) فعليها أولاً أن تصنف هذه الأداة بوضعها في مكانها الصحيح من النموذج الأمني. و" وحدة تنفيذ السياسة الأمنية "، التي تقع في موضع القلب من النموذج الأمني، هي التي تحدد العلاقة بين " المعلومة " و" طالب المعلومة "، فقد تسمح السياسة الأمنية لطالب المعلومة، إن كان جهاز خدمة (Server) مثلاً، بالوصول إلى معلومة معينة، ولتكن قاعدة بيانات الموظفين مثلاً، بعد تعريف " الخادم " لنفسه بشكل صحيح. وقد تكون السياسة الأمنية هي عدم السماح لموظفي الشركة بالدخول إلى ملف المبيعات، ولكن يتم السماح لموظفي كل فرع بالدخول على ما يخص فرعهم فقط.

يبين الشكل (٤-٤) مخططًا عامًا للنموذج الأمني للمؤسسة، ولنأخذ كلاً من هذه المكونات على حدة.

شكل (٤-٤)
النموذج الأمني للمؤسسة



(١) " **طالب المعلومة** ": هذا المكون قد يكون خادمًا (Server)، أو برنامجًا في جهاز حاسب شخصي، أو أحد المستفيدين، أو شبكة أخرى مرتبطة بالشبكة موضع الحماية...إلخ. ويقدم " طالب المعلومة " طلب المعلومات إلى " وحدة تنفيذ السياسة الأمنية " التي تطالبه بتحديد شخصيته قبل الاستجابة لطلبه.

(٢) " **المعلومة** ": قد تكون المعلومة قاعدة بيانات، أو برنامجًا مطلوبًا تنفيذه، أو شبكة خارجية متصلة بالشبكة موضوع الحماية، أو جهاز خدمة آخر، أو خادم الشبكة المرتبط بشبكة الإنترنت. وقد يتبادل " طالب المعلومة " موقعه مع " المعلومة " في بعض الأحيان، فكما تطلب شبكة أخرى معلومات عن شبكتنا فقد تفعل شبكتنا الشيء نفسه لطلب المعلومات من الشبكة الأخرى. و" المعلومة " عليها كذلك أن تتأكد من هوية من يطلب منها المعلومات، بل إن ما يميز السياسة الأمنية القوية هو أن يتم التأكد من هوية " المعلومة " قبل الحصول منها على المعلومات.

(٣) " **وحدة تنفيذ السياسة الأمنية** ": هذه الوحدة نجدها الآن جزءًا من نظم التشغيل، وهي الوحدة المسئولة عن معالجة أي طلبات ترد من " طالب المعلومة "، والتحقق من شخصيته باستخدام " نظام التحقق من الشخصية "، وتسجيل كل

وقائع طلب المعلومات باستمرار باستخدام " نظام المراقبة وتسجيل الوقائع ". وتستعين هذه الوحدة باستمرار بـ " قواعد السياسة الأمنية " المسجلة في قاعدة بيانات النظام.

(٤) " **نظام التحقق من الشخصية** ": هذا النظام الفرعي هو الأداة التي تستخدمها " وحدة تنفيذ السياسة الأمنية " للتحقق من شخصية " طالب المعلومة "، وقد يستخدم هذا النظام الفرعي مجموعة من البرامج لتنفيذ عمليات التحقق من الشخصية، وقد يستخدم جدار حماية؛ فقد تقرر المؤسسة أن هذا المكان هو أنسب مكان لجدار الحماية بدلاً من أن يكون مقر جدار الحماية في وحدة تنفيذ السياسة الأمنية كما يحدث في كثير من الأحوال.

(٥) **نظام المراقبة وتسجيل الوقائع:** هذا النظام الفرعي تستخدمه وحدة تنفيذ السياسة الأمنية لتسجيل وقائع الدخول والاستخدام والاستعلام، كما تستخدمه كذلك لمراقبة تنفيذ السياسة الأمنية والتأكد من عدم حدوث اختراقات للشبكة. وقد يتضمن هذا النظام الفرعي نظاماً لكشف الاقتحام كجزء منه.

(٦) **قواعد السياسة الأمنية:** هنا يمكن أن تحتفظ المؤسسة بقواعد العمل (Business rules) لتي تحدد السياسة الأمنية للمؤسسة، والتي يتم الرجوع إليها بواسطة " وحدة تنفيذ السياسة الأمنية " كلما احتاجت هذه الوحدة إلى اتخاذ قرار بشأن أحد طلبات المعلومات. ويمكن تعديل وإثراء هذه المجموعة من القواعد، كما يمكن أن يوضع جهاز خادم البروكسي في هذا الموضع من النموذج لأنه عادة يحتوي على القواعد التي تتطلب السياسة الأمنية تطبيقها.

٤-٣-٢ اهتمامات الإدارة العليا:

إذا أهمل مسئول أمن المعلومات اهتمامات الإدارة العليا عند تحديده لاحتياجات المؤسسة من البيئة الآمنة، فإنه إما لن يحظى باعتماد السياسة الأمنية التي سيتوصل إليها، أو لن يحظى بالدعم الكافي من جانب الإدارة العليا خلال مراحل التنفيذ، مع ما

تتطلبه هذه المراحل من قرارات مالية وإدارية تظهر فيها الحاجة بشدة إلى الإدارة العليا. فما هي اهتمامات الإدارة العليا فيما يخص الاحتياجات الأمنية للمؤسسة؟ يمكن أن نلخص هذه الاهتمامات في أربع نقاط أساسية.

٤-٣-٢-١ وجود مبررات قوية للميزانية المطلوبة:

الأمن لا يمكن تحقيقه (مجانًا)، فتصميم نظام لكشف الاقتحام مثلاً سيكلف مبلغًا لا يقل عن خمسين ألف ريال، وقد يتطلب الأمر تعديلات في الشبكة ترفع المبلغ إلى مائة وخمسين ألف أو مائتي ألف ريال. هذا فقط لكشف الاقتحام، أما لكي نضيف جدران الحماية وخادم البروكسي وبعض برامج الحماية من الفيروسات فإن الميزانية لهذا الموضوع ستتجاوز بالتأكيد المليون ريال لشبكة كبيرة. هنا لابد من تقديم المبررات للإدارة العليا لكي تقتنع بضرورة اعتماد هذه المبالغ، وهنا يجيء دور مسئولي أمن المعلومات وتقديراتهم فيما يخص الخسارة المالية المتوقعة التي تحدثنا عنها في بداية هذا الفصل. فإذا كانت الخسارة المتوقعة تفوق بكثير هذا الرقم.. فالمبرر موجود وسهل ومقنع، وإلا فلا يمكن إقناع الإدارة العليا بإنفاق مليوني ريال لحماية أصول لا تتجاوز قيمتها عشرة آلاف ريال!!

٤-٣-٢-٢ عدم تجاوز الميزانية المرصودة:

يهم الإدارة العليا بشكل كبير ألا يتم تجاوز الميزانية المرصودة، وأنا في الحقيقة لا أعلم مشروعًا لم يتجاوز الميزانية المرصودة له، بصورة أو بأخرى ! ولذلك فأنت دائمًا تجد الشك في عيون من هم في مواقع الإدارة العليا عندما تحدثهم عن الميزانية المطلوبة للمشروع، وأول ما يبادرونك به هو التأكد من أن الأرقام المطروحة لن تكون قابلة للزيادة. وفي هذه الحالة يمكن مثلاً أن يتم شراء أجهزة الحاسب الشخصي المخصصة لكشف الاقتحام من أحدث طراز، ثم بعد عام يتم استبدالها واقتناء أجهزة أحدث، مع توزيع الأجهزة القديمة على بعض المستفيدين. وهكذا يمكن من خلال

استخدام الميزانية العادية للإمداد بالحاسبات الشخصية تطوير أجهزة أمن المعلومات دون أن يكون هناك إضافة أو عبء زائد على ميزانية المؤسسة.

٤-٣-٢-٣ إدخال التطور التقني دون إرباك المؤسسة:

الجميع، بما فيهم نحن الداعون إلى استخدام التقنية، يخافون التغيير ويخشون من النتائج التي قد تترتب عليه. حتى موروثاتنا الشعبية تدعونا إلى التمسك بما نعرف لأنه (دائماً!) خير من الجديد الذي لا نعرفه، واعتقادنا الجازم (وهو اعتقاد صحيح) بأن كل جديد، كما يحمل المزايا، فهي ليست مزايا بلا ثمن، وإنما هناك ثمن ما يتعين دفعه، ونخشى أن يكون الثمن باهظاً. وإدخال النظم الأمنية في أي مؤسسة غالباً ما يغير من تهيئة الشبكة وخوادمها، وقد يؤدي إلى إعادة تمركز العديد من الأجهزة، وقد يتطلب برامج تكتب، وبرامج يعاد كتابتها.

كما أن إدخال هذه النظم سوف يغير من مسئوليات ومن سلوكيات بعض الموظفين، إن لم يكن جميعهم، فالأدوات التي يتم تركيبها كأجهزة كشف الاختراق أو خادم البروكسي مع ما يصاحبهما من وسائل تسجيل الوقائع، هذه الأدوات قد تكشف بعض الممارسات الخاطئة من جانب بعض المستفيدين أو المسئولين عن الشبكة. قبل تركيب هذه الوسائل الأمنية فإن هذا الموظف يمارس هوايته في أمان دون خشية من رقيب، ولكن افتضاح أمره سيجعل الكثيرين من الموظفين يراجعون تصرفاتهم.

سيتطلب إدخال هذه النظم المزيد من تعديل السياسات والإجراءات، وما ستكتشفه هذه الأجهزة يجب أن يعالج بحكمة، ففي البداية يفضل تنبيه الموظف المخطئ مرة واثنتين قبل إبلاغ الإدارة. فنحن نفترض أن الخطأ، إن وقع من جانب الموظف، فهو ليس جريمة تعمد ارتكابها، ولكنه خطأ يجب أن يوضع في إطاره وألا يعطي حجماً أكبر من حجمه.

٤-٣-٢-٤ اتفاق السياسة الأمنية مع السياسة العامة للمؤسسة:

من الخطأ أن يتم وضع السياسة الأمنية بمعزل عن السياسة العامة للمؤسسة، وإلا فهناك احتمال وقوع التعارض أو التضارب أو عدم التنسيق في أحسن الأحوال، وهذه من الأمور التي تهتم بها الإدارة العليا. بنفس المنطق، فإن أي جهاز يتم تركيبه في الشبكة لابد أن يتوافق مع باقي الأجهزة، وأي إجراء يتم تصميمه لكي يتبع بواسطة الموظفين لابد أن يتوافق مع باقي الإجراءات التي تتبعها المؤسسة.

٤-٣-٣ الأصول المطلوب حمايتها:

عندما تتصل أي شبكة بالإنترنت فإنها تعرِّض ثلاثة من أهم مواردها للخطر، وهي البيانات والحاسبات وسمعة المؤسسة. ولذلك فمن أهم احتياجات أي مؤسسة من السياسة الأمنية هو حماية هذه الموارد الثلاثة.

٤-٣-٣-١ البيانات:

عندما نتكلم عن حماية البيانات فنحن نعني حماية سريتها، وسلامتها، وتوفرها عند الحاجة إليها. فكثير من المؤسسات تحفظ كثيرًا من بياناتها السرية على أجهزة الحاسب فيها وأجهزة الخدمة في شبكاتها، وهذه البيانات تتضمن خطط وتصميمات وميزانيات. في هذه الحالة يكون من الحكمة فصل هذه الأجهزة التي تحتوي على هذا النوع من البيانات عن شبكة الإنترنت. ولكن ماذا لو كانت المؤسسة تمارس " التجارة الإلكترونية " وتحتاج إلى السماح للجمهور بالدخول إلى بعض هذه البيانات من خلال شبكة الإنترنت؟ إذًا هي السياسة الأمنية فقط التي سوف تحمي البيانات وليس العزل. فليس كل جمهور المتعاملين هم من العملاء الطيبين ذوي النوايا الحسنة. ومن المهم للمؤسسة أن تضمن توافر البيانات عند الحاجة إليها، سواء من جانب جمهور المتعاملين معها عبر الإنترنت، أو من جانب الموظفين على الشبكة الداخلية.

٤-٣-٣-٢ أجهزة الحاسب:

حتى لو كانت البيانات التي تحتفظ بها المؤسسة عديمة القيمة، فعلى الأقل لا يجب أن تسمح هذه المؤسسة بإساءة استغلال أجهزة الحاسب لديها، فالمهاجمون قد يستخدمون حاسبات المؤسسة خلال الليل، وقد يقول قائل: " وماذا يهم إذا كانوا يستخدمون الأجهزة في غير وقت الذروة؟ وماذا يضير المؤسسة من ذلك؟ ". والأخطر من ذلك أن أجهزة المؤسسة قد يتم استغلالها للهجوم على مؤسسات أخرى مما قد يسبب الحرج البالغ للمؤسسة، علاوة على التبعات القانونية.

٤-٣-٣-٣ سمعة المؤسسة:

ما ذكرناه في الفقرة السابقة من احتمال استغلال أجهزة المؤسسة كنقطة وثوب لاقتحام شبكات أخرى قد يكون كافياً للإساءة إلى سمعة المؤسسة، فأصابع الاتهام في هذه الحالة ستشير إليها. وفي بعض الوقائع تم إرسال رسائل إلكترونية مزورة باسم أستاذ جامعي لمجموعة من الشخصيات مليئة بالشتائم، الأمر الذي استدعى وقتاً وجهداً ومالاً من هذا الأستاذ لمحو آثار هذه الرسائل المزورة. وحدث أيضاً أن قام طالب بتزوير رسالة بريد إلكترونية باسم أستاذه لجميع الطلاب تلغي اختبار منتصف العام الذي كان موعده في اليوم التالي. ولم يحضر الاختبار سوى عدد محدود من الطلاب (الذين لا يقرأون بريدهم الإلكتروني !) وبالطبع أثر ذلك على مصداقية استخدام البريد الإلكتروني في الكلية ومن ثم على سمعة الكلية.

٤-٤ السياسة الأمنية:

تبين لنا من القسم السابق أهمية السياسة الأمنية للمؤسسة والضوابط التي يجب أن تتوفر فيها. واعترف أنني إلى عهد قريب كنت أعتقد بضرورة وجود كتيب واحد مطبوع بشكل أنيق ومنشور على مستوى المؤسسة يحتوي على السياسة الأمنية لهذه المؤسسة بالكامل، وأن هذا الكتيب (وكنت عادة أسميه " الخطة الأمنية الشاملة

للمعلوماتية ") لابد أن يشمل كل شيء يخص السياسة الأمنية، بدءًا من إجراءات منح الصلاحية لموظف، مرورًا بسياسة استخدام شبكة الإنترنت، وضوابط الأمن في برامج التطبيقات، إلى خطة مواجهة الكوارث. ولكن التجربة وحدها علمتني أن هذا أمر صعب للغاية، إن لم يكن مستحيلاً من الناحية العملية. ولذلك فأعتقد أنه من المقبول أن تكون السياسة الأمنية موزعة و(مدمجة) ضمن سياسات وإجراءات المؤسسة، وأنه ليس من الضروري أن تطبع وتوزع، ذلك لأنها قابلة للتعديل والإضافة والحذف باستمرار، والسبب في ذلك ببساطة هو أن السياسة الأمنية تدس أنفها في كل شيء. كيف تقنع المستفيد بأن كلمة السر الخاصة به يجب أن تتغير بشكل دوري؟ وكيف تقنعه بأن الكلمة التي يختارها يجب أن تكون صلبة في مواجهة أساليب الهندسة الاجتماعية لكسر كلمات السر؟ فيبتعد عن أسماء أولاده وتواريخ ميلادهم، بل يجب أن يبتعد عن أي كلمة ترد في قاموس اللغة الإنجليزية؟ هذا مجرد مثال يبين صعوبة فرض السياسة الأمنية، فضلاً عن صياغتها ومراجعتها وإعدادها في صورتها النهائية. ولكن، من ناحية أخرى، فإن إعداد السياسات الأمنية مسبقًا يوفر الكثير من الجهد والمناقشات مع المستفيدين فيما بعد.

من المهم أن نوضح أن السياسة الأمنية " المثالية " قد تطبع وتوزع، ولكن تطبيق هذه السياسة الأمنية شيء آخر يتوقف كثيرًا على ثقافة المستفيدين وطبيعة العلاقات داخل المؤسسة. فمن الطبيعي أن تجد السياسة الأمنية تركز على أن الموقع يجب أن يكون منيعًا وألا يمكن اختراقه بأي صورة من الصور، وأن كل مستفيد يكون له حساب واحد فقط، وأن الحساب الواحد لا يشترك فيه أكثر من مستفيد، وأن اختيار كلمات السر لابد أن يتم بعناية. كل هذا عظيم.. ولكن المهم تطبيقه وفرض تنفيذه على العاملين.

٤-٤-١ متطلبات السياسة الأمنية:

على السياسة الأمنية للمؤسسة أن تحقق المتطلبات التالية:

١- أن تكون تكلفتها معقولة أو مناسبة.

٢- أن تكون القيود معقولة بحيث لا تمنع المستفيدين من استخدام أجهزة الحاسب لديهم.

٣- أن تتوافق مع أسلوب أداء الموظفين لأعمالهم وتعاملهم مع العالم الخارجي.

٤- أن تلبي الاحتياجات القانونية للموقع، وأن تراعي العوامل القانونية والإجرائية. ولذلك ففي أحيان كثيرة يتم التضحية ببعض المتطلبات الأمنية اليسيرة في مقابل تيسير سير العمل في المؤسسة، وهذا أمر لا غبار عليه.

٤-٤-٢ سمات وثيقة السياسة الأمنية:

لما كانت السياسة الأمنية المكتوبة للمؤسسة موجهة بالدرجة الأول للمستفيدين وللإدارة العليا كي يسترشد بها كل من الفريقين عند اتخاذه لقرارات العمل، فإن وثيقة السياسة الأمنية يجب أن تتسم بالصفات التالية:

(١) **الوضوح الكامل:** يجب أن تكون السياسة الأمنية واضحة ومفهومة، وأن تكون مجموعة القيود والإجراءات والقواعد التي تحتويها مبررة ومقنعة، حتى يتبعها الجميع عن اقتناع، وحتى يمكن الاستمرار في اتباعها حتى عند رحيل واضعيها.

(٢) **تحديد مسئوليات كل شخص:** يجب أن تحدد السياسة الأمنية بكل وضوح المسئوليات والواجبات الملقاة على عاتق كل موظف وكل مسئول وكل مستفيد، فلا يجب أن تركز فقط على ما يجب وما لا يجب على المستفيد فعله، فهي بهذا الشكل تكون عدائية وغير عادلة. ولا يجب من ناحية أخرى أن تركز فقط على مسئوليات مسئولي أمن المعلومات، فإن ذلك سيعطي انطباعاً بأن هناك من يتولى مسئولية الأمن، وأن دور المستفيد هو دور هامشي.

(٣) **استخدام لغة بسيطة:** المستفيدون في المؤسسة ليسوا كلهم من خبراء أمن المعلومات، ومن ثم فلابد أن تكون اللغة المكتوبة بها السياسة الأمنية لغة بسيطة لا تحتوي على الكثير من المصطلحات، وأن يكون هناك شرح واضح لكل مصطلح

فني يتم تداوله في الوثيقة، فلن نتوقع تعاون المستفيد في تنفيذ ما لا يفهمه!

(٤) **سلطة فرض السياسة:** كما أوضحنا من قبل، فإن أهم شيء هو فرض تنفيذ السياسة الأمنية وليس فقط كتابتها أو توزيعها. لذلك يجب أن تتضمن وثيقة السياسة الأمنية تحديد من لديهم صلاحية حرمان المستفيد من الخدمة عند المخالفة، وتحديد من لديهم صلاحية إيقاف بعض الخدمات المقدمة إذا كانت تؤثر على أداء الشبكة أو أمن المعلومات فيها.

(٥) **إتاحة المجال للحالات الخاصة:** لأنه لا توجد سياسة أمنية تغطي كل احتمالات الحاضر والمستقبل معاً، فيجب تحديد أسلوب تعديلها للسماح بالاستثناءات، عندما تظهر حالات خاصة تستدعي ذلك، وهل تمنح صلاحية تحديد الاستثناءات لشخص معين؟ أم للجنة من عدة أشخاص؟

(٦) **إتاحة المجال للمراجعة:** لابد من إتاحة المجال لمراجعة السياسة الأمنية وتنقيحها عبر الزمن، ومع ظهور مستجدات جديدة، وتقنيات جديدة، وظروف جديدة، كأن يزداد عدد العاملين أو تزداد سعة وسرعة الخطوط المتاحة، أو تدخل المؤسسة إلى مجال جديد كالتجارة الإلكترونية مثلاً.

٤-٤-٣ ما يجب أن تحتويه وثيقة السياسة الأمنية:

يجب أن تتعرض السياسة الأمنية للمؤسسة للنقاط التالية:

- تعريف المستفيد وتحديد من له الحق، من بين موظفي المؤسسة، في الحصول على حساب مستفيد، وهل يسمح بوجود حساب ضيف (Guest account)؟ وما هو موقف العاملين غير الدائمين كالمتعاقدين وممثلي الشركات الأخرى وعملاء المؤسسة وغيرهم؟
- هل يسمح بالاشتراك في حساب واحد بين مجموعة من الأشخاص؟ وماذا عن السكرتير الذي يستخدم حساب المدير ليتعامل مع بريد المدير الإلكتروني؟ وماذا عن المشروعات المشتركة التي يشترك فيها أكثر من مستفيد؟ وماذا عن أفراد العائلة؟

أي عن استخدام الزوجة والأولاد لحساب الموظف للاتصال بالإنترنت من المنزل مثلاً؟

- متى يجب إغلاق حساب المستفيد؟ في حالات الاستقالة أو الانتقال إلى عمل آخر مثلاً. وماذا يجب أن يتم فعله في هذه الحالة؟ هل يتطلب الأمر نموذج إخلاء طرف مثلاً؟
- مَن مِن المستفيدين يسمح له بتركيب جهاز " مودم " في حاسبه الشخصي للاتصال الخارجي؟ وهل يمكن تعميم ذلك لمن يشاء؟
- ماذا يجب على المستفيد اتخاذه من الإجراءات قبل توصيل جهاز الحاسب الخاص به بشبكة المؤسسة؟
- ما هي درجة الأمن التي يجب أن يكون عليها الحاسب الشخصي الذي يمكن من خلاله الحصول على الخدمات من أحد خوادم الشبكة؟
- ما هي درجة الأمن التي يجب أن يكون عليها الحاسب الشخصي قبل أن يرتبط بشبكة أخرى، إذا كانت هذه الشبكة مرتبطة بالإنترنت ارتباطاً غير مؤمَّن؟
- ما هو الأسلوب المتبع لحماية المعلومات المالية الخاصة بالمؤسسة؟
- كيف سيتم حماية المعلومات الحساسة الخاصة بالموظفين أو العملاء؟ وهل تحتاج فروع المؤسسة في الخارج إلى تعديلات في السياسة الأمنية وفقاً لقوانين البلد التي توجد به؟
- ما هو المطلوب اتباعه من جانب المستفيدين الأفراد لحماية أنفسهم وموقعهم؟ وما هي شروط كلمة السر التي يجب على المستفيد استخدامها؟ وما هو المعدل الذي يجب أن يغير به كلمة السر؟
- ما هي حدود المسموح باستخدامه على شبكة الإنترنت؟ وهل يمكن للمستفيدين استقبال ملفات من الإنترنت وتشغيلها على أجهزتهم؟ أم عليهم تمريرها أولاً على نظام كشف الفيروسات؟

- ما هي الاحتياطات التي يجب اتخاذها لحماية أجهزة الشبكة من الفيروسات؟
- من المسئول عن ربط موقع المؤسسة بالشبكات الخارجية؟ وما هو تعريف المؤسسة للشبكات الخارجية؟ هل من حق مديري المشاريع أن يربطوا موقع المؤسسة بمواقع أخرى ترتبط بالمشروعات التي يديرونها؟ وما هي الصلاحيات التي تمنح لموظفي هذه المواقع المشاركة للمؤسسة؟ وماذا عن الروابط التي تتم مع شبكة الإنترنت؟
- إلى أي مدى يتم تأمين أجهزة الحاسب الخاصة بالموظفين في منازلهم؟ وكيف سيتم تأمين اتصالهم بشبكة المؤسسة؟ ما هو أسلوب التحقق من شخصيتهم عند دخولهم عن بعد إلى شبكة المؤسسة!.
- كيف يستطيع الموظفون الذين يغادرون مقر العمل في إجازة أو مهمة رسمية أن يتصلوا بشبكة المؤسسة؟ وهل سيكون من حقهم الحصول على بريدهم الإلكتروني فقط؟ أم سيسمح لهم باستخدام حاسباتهم الشخصية عن بعد؟
- ما هي المتطلبات التي يلزم توافرها في الأجهزة التي قد تستخدم في مشروع التجارة الإلكترونية أو الحكومة الإلكترونية؟
- ما هي المعلومات التي تعتبر من أسرار المؤسسة؟ وكيف سيتم حماية هذه المعلومات السرية؟ وهل يسمح بإرسالها خارج الشبكة المحلية من خلال البريد الإلكتروني؟
- إذا كان للمؤسسة مواقع بعيدة (Remote sites) فكيف يمكن لهذه المواقع أن تجري اتصالاً آمناً مع شبكة المؤسسة الرئيسية.

٤-٤-٤ ما لا يجب أن تحتويه وثيقة السياسة الأمنية:

- لا يجب أن تظهر الوثيقة الأمنية التفاصيل الفنية لكيفية حماية الأصول، أو لكيفية الحماية من الفيروسات، أو أسلوب عمل جدار الحماية أو خادم البروكسي، أو غير ذلك من التفاصيل التي قد تؤدي معرفتها إلى تسهيل مهمة المهاجمين لشبكة المؤسسة.

- تختلف السياسة الأمنية من مؤسسة لأخرى، فلكل مؤسسة مخاطر معينة تود مكافحتها، كما أن لها قيوداً مختلفة، وطبيعة مختلفة للمستفيدين، وقدرات مالية مختلفة. يؤدي كل ذلك إلى اختلاف السياسة الأمنية من مؤسسة لأخرى، بل إلى اختلاف السياسة الأمنية لنفس المؤسسة عبر الزمن بنمو المؤسسة وتغير احتياجاتها. ولذلك لا يجب أن تعكس السياسة الأمنية للمؤسسة سياسة مؤسسة أخرى أو تقليداً لجهة أخرى.
- لا يجب أن تتعرض وثيقة السياسة الأمنية لأشياء لا تمس صميم أمن المعلومات، فقيام بعض المستفيدين بعرض صور خليعة مثلاً على شاشات أجهزتهم أمر لا دخل للسياسة الأمنية فيه. قد يدخل هذا الأمر في باب الآداب العامة أو سوء استخدام مكان العمل، ولكن لابد أن نركز عند تحديد ما هو المباح وما هو الممنوع على ما يؤثر على أمن المعلومات فقط دون غيره. فلا يعنينا هنا أن يستخدم الموظف جهاز الحاسب في ألعاب الكمبيوتر أو المحادثة مع الآخرين. بل يجب أن نهتم بكيفية اتصاله بالآخرين، وهل هذا الاتصال مؤمن أم لا.

الفصل الخامس
أساليب انتهاك شبكات المعلومات



في الفصل السابق تحدثنا عن متطلبات الأمن في شبكات المعلومات، وعن المخاطر التي تواجهها هذه الشبكات، وحاجتها لسياسة أمنية تتصدى لهذه الأخطار. وننتقل في هذا الفصل إلى شرح أساليب انتهاك شبكات المعلومات، وكيفية مقاومتها بتطبيق السياسة الأمنية السابق ذكرها.

تتعدد أساليب انتهاك شبكات المعلومات، وتهدف هذه الأساليب إلى مهاجمة هذه الشبكات وتحقيق نفع معين للمهاجم من وراء ذلك، وفي بعض الأحيان لا يكون هناك نفع للمهاجم سوى تعريض الموقع الضحية للخطر وللضرر. وسوف نحاول في هذا الفصل تصنيف أساليب انتهاك شبكات المعلومات. فنعرض للتنصت، الذي يتم إما عن طريق مراقبة الرسائل (Packet sniffing)، أو عن طريق إعادة إرسال هذه الرسائل (Replay) بهدف سرقة المعلومات. وسنتعرف على كيفية مقاومة هذا الأسلوب إما بتشفير الملفات المنقولة عبر الشبكة، أو بتشفير قناة الاتصال نفسها.

ثم نتعرض لأسلوب إقحام الرسائل وتزوير المعلومات، وكيف تتم مهاجمة الخادم باستخدام الأوامر، أو مهاجمة البيانات نفسها. وكيف يمكن التحقق من سلامة الرسائل باستخدام المجموع الاختباري (Checksum) أو القيمة الاختبارية (Hash).

ثم نتعرض لاقتحام المواقع فنحدد وسائل هذا الاقتحام، ونتحدث عن الاقتحام العشوائي، وعن الأبواب الخلفية التي تترك مفتوحة عمداً في بعض النظم والأجهزة، وعن انتحال الشخصية، واختطاف المواقع. ثم نتحدث عن اعتراض البث، والأساليب التي تستخدم في تنفيذه.

نتحدث بعد ذلك عن عرقلة الخدمة (Denial of service) كأحد أكثر الأساليب انتشاراً، والذي يتم إما بالإغراق بالبيانات، أو باستغلال ثغرات السياسة الأمنية للمواقع، أو بالتعاون بين مجموعة من المهاجمين. ونتحدث عن بعض أنواعه مثل هجوم " قطرة الدمع "(Teardrop attack).

وفي نهاية الفصل نقدم سيناريو كاملاً لعملية اقتحام ناجحة نستخدم فيها، كمثال،

موقع معهد الإدارة العامة، ولكننا حرصنا ألا نصل إلى الحد الذي يستخدم فيه المهاجمون هذه المعلومات لتعريض الموقع للخطر. فنتحدث عن المراحل التي يمر بها الهجوم وهي مرحلة جمع المعلومات، ثم مرحلة فحص الشبكة بهدف التعرف على النظم التي تحتويها، والتعرف على الخدمات التي تقدم على هذه النظم، ومعرفة نقاط الضعف أو الثغرات التي يمكن من خلالها مهاجمة هذه الشبكة، ثم في النهاية مرحلة الهجوم الفعلي الذي بدأنا الفصل بتوضيح أنواعه.

٥ـ١ التنصت:

المقصود بالتنصت هو قيام المهاجم أو المقتحم (Hacker) بمراقبة ما يدور في الشبكة، وما يتم تبادله فيها من رسائل، وذلك بهدف الحصول على معلومات يهتم الضحية بإبقائها في طي الكتمان. يتم ذلك عن طريق مراقبة حزم الرسائل المارة بالشبكة (من أي نقطة بين موقع الضحية والمواقع البعيدة التي يتعامل معها)، ويلتقط المهاجم الرسائل غير المشفرة التي يعثر عليها. وهناك نوعان من التنصت:

- الأول هو " مراقبة الرسائل "(Packet sniffing)
- والثاني هو " إعادة إرسال الرسائل " (Replay)

٥ـ١ـ١ مراقبة الرسائل (Packet sniffing):

ما نطلق عليه (Sniffing) هو ما يفعله الكلب حين يتشمم لفافة ما ليحاول معرفة ما بداخلها. وهناك برامج حديثة تتولى مراقبة حزم الرسائل وتفعل ذلك بشكل آلي يعفي المهاجم من التدخل بنفسه.

عادة يسعى المهاجم من خلال " مراقبة الرسائل " (Packet sniffing)، إما وراء كلمات السر، أو وراء بعض المعلومات الحساسة التي يتوقع وجودها داخل الرسالة. ولكل من هذين الهدفين أسلوب مختلف في مواجهته؛ فحماية كلمات السر من المهاجم

الذي يستخدم أسلوب مراقبة الرسائل أمر سهل، إذ يمكن استخدام إحدى وسائل التحقق من الشخصية (Authentication) لكشف شخصية المهاجم، ويمكن اللجوء إلى الأسلوب الناجح الذي يستخدم البطاقة التي تسمح باستخدام كلمة السر لمرة واحدة (Onetime password hardware)، وهذه البطاقة لا يتجاوز حجمها حجم الآلة الحاسبة الصغيرة. وبعد تركيب البرنامج اللازم على جهاز الحاسب، على المستفيد الراغب في الدخول إلى الجهاز أن يستخدم كلمة السر التي تولدها هذه البطاقة بشكل عشوائي، وفي كل مرة تولد البطاقة كلمة سر جديدة. ولتفادي اختراق النظام عند سرقة البطاقة، لا يتم السماح باستخدام البطاقة نفسها إلا بواسطة كلمة سر أخرى يجب أن يقوم المستفيد بإدخالها خلال فترة زمنية قصيرة. وباستخدام هذا الأسلوب لا يهم إن استطاع المهاجم الحصول على كلمة السر، لأنها لن يكون لها قيمة بعد ذلك.

أما حماية المعلومات من مراقبي الرسائل (Sniffers) الذين يسعون وراء المعلومات التي تحتويها الرسالة فهو أمر أكثر صعوبة. فالحماية هنا تتم باستخدام التشفير، إما بتشفير الملفات التي سيتم نقلها، أو بتشفير قنوات الاتصال (Communication links) نفسها.

٥-١-١-١ تشفير الملفات:

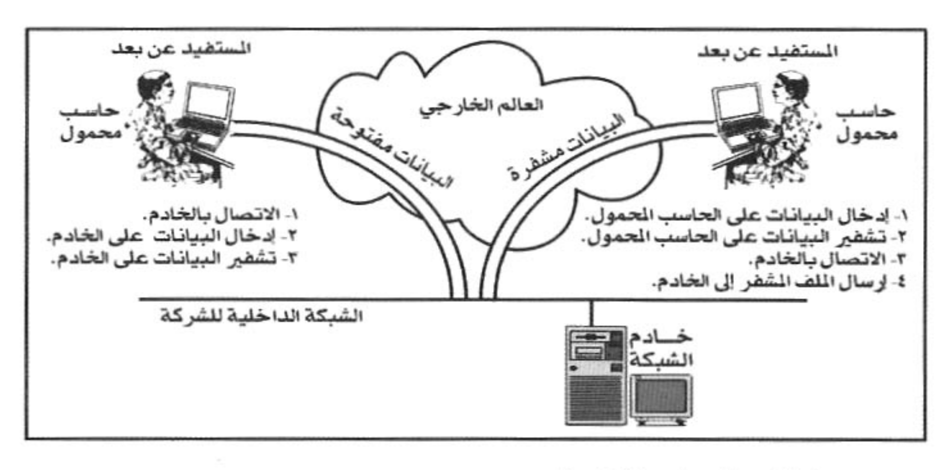
نلجأ لتشفير الملفات إذا كان المستفيد ينقل ملفات كاملة مثل إرسال البريد (SMTP)، أو نقل الملفات (FTP)، وبشرط أن يكون لدى المستفيد وسيلة آمنة لإدخال المعلومات التي ستستخدم في تشفير هذه الرسائل، وبشرط أن يكون لديه أيضاً وسيلة آمنة لإيصال المعلومات اللازمة لفك التشفير إلى الطرف الآخر الذي سيستقبل الملف. ويكون تشفير الملفات حتمياً إذا كان الملف سيمر بعدة قنوات اتصال ليست جميعها محل ثقة، أو إذا كان الملف سيبقى لفترات طويلة في بعض الأجهزة المستضيفة (Hosts) غير الموثوق بها. والحالات التي يناسبها هذا الأسلوب هي عندما يستخدم المستفيد حاسباً محمولاً (Portable)، ويقوم بكتابة بياناته السرية على هذا الحاسب، ويقوم بتشفير البيانات على الحاسب المحمول نفسه، باستخدام أحد نظم التشفير التي

تستخدم المفتاح العلني (Public key encryption system) يقوم المستفيد بكل ذلك قبل الاتصال عن بعد بخادم الشبكة، ثم يتصل بالشبكة ويقوم بعد ذلك بإرسال الملف المشفر بأمان تام، حتى لو مر الملف بالعديد من خوادم البريد (Mail servers) غير المأمونة، أو بخطوط الاتصال غير المعروفة.

ولكن تشفير البيانات لن يفيد كثيرًا في حالة دخول المستفيد عن بعد أولاً إلى خادم الشبكة من خلال حاسبه المحمول، ثم قيامه بعد ذلك بكتابة البريد ومن ثم تشفيره. في هذه الحالة يستطيع المهاجم مراقبة المستفيد خلال كتابته للرسالة البريدية، بل إنه سيكون في مقدوره التقاط بعض المعلومات السرية المستخدمة خلال عملية التشفير، مثل مفتاح التشفير، ذلك لأن البريد وما يصاحبه من معلومات تمر من حاسب المستفيد إلى خادم الشبكة مفتوحة و غير مشفرة كما يبين الشكل (٥-١).

شكل (٥-١)

المستفيد عن بعد قد يتصل بخادم الشبكة اتصالاً مفتوحًا



٥-١-٢ تشفير قنوات الاتصال:

في أحوال كثيرة، قد يكون من الأفضل من الناحية العملية، أن نقوم بتشفير عملية

المحادثة بأكملها بدلاً من تشفير البيانات عند إرسالها. ويتم ذلك بأن يقوم المستفيد بالتشفير من خلال اللجوء إلى استخدام الشبكة الخاصة الافتراضية (VPN)، والتي سوف نتعرض لها بالتفصيل في الفصل العاشر، ويستخدم " خادم التشفير " (Encryption server) عند مداخل المواقع التي تضمها الشبكة الافتراضية. أو قد يلجأ المستفيد إلى استخدام بروتوكول مشفر بالفعل، مثل بروتوكول (SSH).

وفي هذه الأيام تنتشر على شبكة الإنترنت عمليات التنصت (Eavesdropping) من جانب المهاجمين، كما تنتشر من الناحية الأخرى عمليات التشفير من جانب أصحاب الرسائل. إذ يتم اللجوء إلى تشفير جميع المعلومات الواردة من شبكة الإنترنت إلى الشبكة الداخلية، ما لم يكن هناك ما يؤكد أنها معلومات عادية وليست حساسة. وكذلك يتم تشفير جميع المعلومات الصادرة من الشبكة الداخلية إلى الإنترنت، طالما كان هناك ما يدعو إلى الاعتقاد بأنها معلومات حساسة.

لا تستطيع جدران الحماية أن تفعل شيئًا لمنع " مراقبة الرسائل "(Packet sni-ffing)، كما أن الشبكات الخاصة الافتراضية (VPNs) وبروتوكولات التشفير لن تمنع " مراقبة الرسائل " تمامًا، وإنما سوف تقلل من أثرها ومن احتمالات نجاحها.

٥-١-٢ إعادة إرسال الرسائل(Replay):

تعتبر عمليات " إعادة إرسال الرسائل " (Replay) واحدة من أساليب التنصت، فالمهاجم في هذه الحالة يقوم بالتقاط المعلومات عند مرورها ثم يقوم بتخزينها، ثم يعيد إرسالها مرة أخرى فيما بعد.

هناك طريقتان يمكن أن يتم بهما ذلك:

- الأولى يتم فيها اختيار المعلومات التي يتم تخزينها وإعادة إرسالها بشكل انتقائي، وهذه الطريقة تعتمد على قدرة المهاجم على تمييز المعلومات التي يسعى وراءها (مثلما يحدث في حالة سرقة كلمات السر).

– الطريقة الأخرى يتم فيها إعادة إرسال حزم الرسائل كلها دون تمييز.

توجد أنواع كثيرة من التشفير يتم استخدامها للحماية من هذا النوع من الهجوم الذي يهدف إلى جمع المعلومات لإعادة إرسالها. ولكن التشفير لن يفيد إذا كان المهاجم يستطيع تحقيق هدفه بمجرد إعادة استخدام حزمة الرسالة كما هي دون معرفة محتواها، ففي هذه الحالة سوف يتم إعادة الإرسال دون فك الشفرة، بل إن ذلك قد يكون نوعًا من الخداع الناجح للجهة المستقبلة التي تجد الرسالة مشفرة وتفك بنفسها شفرتها فتنخدع بها وتظن أنها رسالة شرعية.

لا يصلح هذا الأسلوب (إعادة إرسال الرسائل) في حالة استخدام بروتوكول (TCP) بسبب وجود الأرقام التسلسلية للحزم في مقدمة الحزمة، وبذلك ينكشف أمر الحزمة التي يعاد إرسالها، ويتم رفضها عند استقبالها. ولكن هذا الأسلوب يصلح في حالة استخدام بروتوكول (UDP).

والحل الوحيد في مواجهة هذا الأسلوب من أساليب التنصت هو استخدام أحد البروتوكولات التي ترفض تمرير الحزم المعاد إرسالها، مثل البروتوكول الذي يستخدم " بصمة التوقيت "(Time stamp)، أو يستخدم الأرقام المتسلسلة في الإرسال. كما يجب أن يقوم البروتوكول المستخدم كذلك بالتحقق من سلامة الرسالة وعدم العبث بها، لمنع المهاجم من تعديل حزمة الرسائل التي يحاول إعادة إرسالها. ويمكن أن يتم هذا التحقق باستخدام أساليب مثل " المجموع الاختباري " (Checksum) وغيره من الوسائل التي تكتشف أي تعديل يكون قد تم على الرسالة.

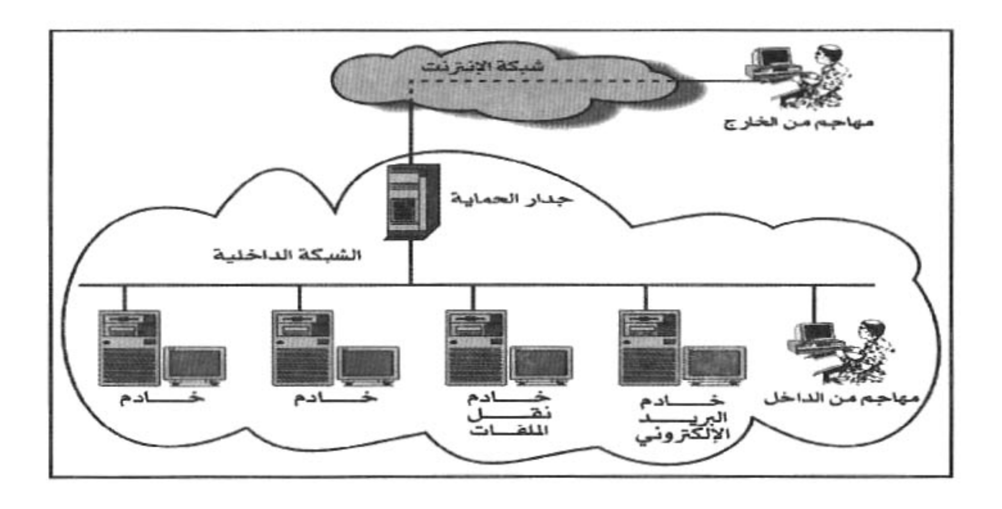
في هذا النوع من أنواع التنصت لا تستطيع جدران الحماية فعل الكثير، ولكن في حالات قليلة، عندما يتم إعادة إرسال الحزمة كما هي (مجرد تكرار الإرسال) فإن بعض مصافي الحزم (Packet filters) قد تستطيع اكتشاف تكرار الرسالة. ويبقى أن نؤكد أن أفضل وسيلة للحماية من عملية إعادة الإرسال (Replay) هي ، كما ذكرنا، استخدام بروتوكول يحتوي على خاصية التأكد من صحة الرسالة، كما يحتوي على بصمة التوقيت.

٥-١-٣ سرقة المعلومات:

من أهم أهداف التنصت هو سرقة المعلومات، ويستطيع المهاجم أحيانًا أن يسرق المعلومات دون أن يتصل مباشرة بجهاز الضحية، بل باستغلال بعض خدمات الإنترنت التي تقدم المعلومات، وذلك باستخراج معلومات أخرى من هذه الخدمات بطرق ملتوية، سنشرحها في نهاية هذا الفصل.

وما جعل الأمر سهلاً أمام المهاجمين هو أن معظم خدمات الإنترنت قد تم تصميمها للاستخدام على الشبكات المحلية (Local area networks)، ومن ثم فهي لا تتضمن مستوى السرية أو نوع السرية الذي يحميها إذا ما تم استخدامها عبر شبكة الإنترنت. وما مهد الطريق أكثر أمام المهاجمين أن الاسم وكلمة السر هي من أسهل المعلومات التي يمكن للمهاجم الحصول عليها، والتي سوف تفتح له الباب بالتالي لسرقة ما يشاء من معلومات (Burns ٢٠٠١) وتزداد مهمة المهاجم سهولة إذا كان مهاجمًا من الداخل لأن رسائله لا تمر بجدار الحماية كما يبين شكل (٥-٢).

شكل (٥-٢)
المهاجم من الداخل لا تمر رسائله بجدار الحماية



تتطلب سرقة المعلومات إما درجة عالية من التركيز والصبر، أو معرفة مكان وتوقيت مرور المعلومات التي تريدها، كأن تعرف مثلاً أن شخصًا ما يتصل بالبنك في الساعة الثانية بعد الظهر من كل أربعاء، لتحويل مبلغ من أحد حسابات الشركة إلى حساب آخر. هنا يمكن التنصت والحصول على الرسالة وتحليلها ومعرفة الكثير من المعلومات، أقلها أرقام الحسابات والرقم السري المستخدم للتحويل بين الحسابات.

كثير من الشبكات تمر بها معلومات لا تخصها، بل تخص شبكات أخرى، ويمكن لأجهزة الشبكة الوسيطة أن (تطلع) على هذه المعلومات. أي أن الرحلة الطويلة للمعلومات عبر شبكة الإنترنت ليست رحلة آمنة، بل محفوفة بالمخاطر من جانب العديد من أجهزة الحاسب في الشبكات الوسيطة. ولذلك فإن شبكات مقدمي الخدمة والشبكات التي توجد بها نظم عمومية، أي الشبكات التي يدخل إليها الجميع، تعتبر هدفًا رائعًا للمهاجمين، فباختراق أي من هذه الشبكات يجد المهاجم نفسه في وسط كم هائل من المعلومات.

كذلك يجب أن نؤكد أن الشركة التي تقرر تقديم خدماتها (أو معلوماتها) عبر شبكة الإنترنت لا يمكن أن تضمن أن هذه المعلومات لن تتسرب إلى شخص غير مقصود، سواء عن طريق انتحال الشخصية أو عن طريق التنصت (Sniffing).

٥-٢ إقحام الرسائل وتزوير المعلومات:

ذكرنا في معرض الحديث عن انتهاك المعلومات بأسلوب " التنصت "، وفي حالة لجوء المهاجم إلى إعادة إرسال الرسائل (Replay)، أن هذا المهاجم قد يقوم بتعديل نص الرسالة التي يريد إعادة إرسالها بحيث يقوم بتزوير ما ورد بها من معلومات.

٥-٢-١ إقحام المعلومات وتعديلها (Data Injection & Modification):

من أجل التمكن من إقحام المعلومات يعمد بعض المهاجمين إلى السيطرة على "

الموجه " (Router) الذي يقع بين كل من " العميل " و" الخادم "، والذي يتحكم في قناة الاتصال الرئيسية بينهما. وفي هذه الحالة يكون في مقدور المهاجم استقبال حزم الرسائل، ثم تعديلها (وليس فقط قراءتها) وإعادة إرسالها، وهو ما نطلق عليه " إقحام المعلومات وتعديلها " (Data injection & modification) وفي أحوال نادرة قد يستطيع المهاجم تحقيق ذلك حتى دون أن يتمكن من السيطرة على " الموجه "، وذلك عن طريق إرسال الحزمة المزورة بحيث تصل إلى وجهتها (قبل) الحزمة الأصلية. في هذه الحالة سيقبل النظام الرسالة المزورة، وعند وصول الرسالة الأصلية سيرفضها النظام ظنًا منه أنها هي المزورة !

تشفير البيانات هنا لن يحل المشكلة، ولن يحمي البريد المار من هذا الأسلوب من أساليب الانتهاك؛ فإن المهاجم سيكون في مقدوره تعديل البيانات المشفرة وتغيير محتواها دون فك الشفرة. والمهاجم لن يستطيع بالطبع أن يتوقع شكل البيانات بعد أن يتم فك شفرتها، ولكنها بالتأكيد، بعد تعديلها من جانب المهاجم، ستكون مختلفة عن البيانات الأصلية. فالتشفير في هذه الحالة سوف يمنع المهاجم من تغيير مبلغ التحويل البنكي مثلاً من ٢,٠٠٠ ريال إلى ٢,٠٠٠,٠٠٠ ريال، ولكنه لن يمنع المهاجم من تغيير الرسالة بشكل يؤدي إلى أن تفقد معناها، بل قد يؤدي الأمر في بعض الأحيان إلى تخريب نظام التطبيقات الذي يستقبل هذه الرسائل في البنك لمعالجتها. وفي إحدى الوقائع التي حدثت مؤخرًا، قام المهاجم (بتخمين) موقع حقل رقم الحساب البنكي من الرسالة في إحدى الرسائل المشفرة الصادرة من مركز البنك الرئيسي إلى أحد فروعه، وقام المهاجم بتغيير هذا الرقم عشوائيًا. وتصادف أن الرقم الجديد كان رقمًا حقيقيًا لحساب آخر بالبنك، وتم تحويل المبلغ إلى الحساب الآخر.

المهاجم في هذه الحالة لم يتمكن من تحقيق أي نفع، ولكنه سبب مشكلة كبيرة للبنك، وربما كان هذا هو ما يهدف إليه. ولكي نحقق الحماية الكاملة من هذا النوع من أساليب الهجوم (إقحام المعلومات وتعديلها) فلن تفيدنا جدران الحماية، وإنما يفيدنا استخدام الشبكات الخاصة الافتراضية (VPN)، وكذلك استخدام بعض أساليب

التحقق من سلامة الرسائل، التي نوهنا عنها سابقًا في هذا الفصل، حيث تتم إضافة قيمة رقمية اختبارية (Checksum) إلى الرسالة. هذه القيمة يتم حسابها من واقع محتويات الرسالة، وبحيث لا يستطيع المهاجم تقليدها بعد تعديل الرسالة.

٥-٢-٢ مهاجمة الخادم:

هناك نوع آخر من الهجوم عن طريق " مهاجمة الخادم باستخدام الأوامر " (Command-channel attack) والذي فيه تتم مهاجمة الخادم مقدم الخدمة بأن ترسل إليه الأوامر بنفس الأسلوب الذي يتلقاها به عادة (من خلال قناة الأوامر). ويتم ذلك إما باستغلال أوامر صحيحة وإرسالها لأداء مهام خبيثة، أو بإرسال أوامر غير صحيحة لا يفهمها الخادم واستغلال الثغرات الموجودة في الخادم عند تعامله مع هذه الأوامر غير الصحيحة.

ومن أشهر الأمثلة على هذا الأسلوب من أساليب انتهاك المعلومات ما اشتهر باسم " دودة موريس " التي انتشرت في شبكة الإنترنت عام ١٩٨٨، والتي هاجمت خدمة (Sendmail) باستخدام أحد أوامر فحص البرامج (Debugging) الذي يظل في العادة متروكًا دون حماية، كما هاجمت هذه الدودة خدمة (Finger) بإمطار الخادم بأوامر يزيد طولها عن الطول المطلوب مما تسبب في إغراق المساحات الوسيطة في الذاكرة. هذا النوع من الهجوم يمكن تجنبه بواسطة جدار الحماية، وذلك بتحديد عدد الأجهزة التي يستطيع المهاجم فتح قنوات أوامر معها، وبتوفير جهاز خدمة مؤمن يرتبط بهذه الأجهزة. وفي بعض الأحيان يستطيع جدار الحماية أن يحجب بعض الأوامر التي يكون من السهل اكتشاف أنها يجب أن تحجب، مثل الأوامر غير الصحيحة، أو الأوامر التي يقرر المستفيد عدم التعامل معها.

٥-٢-٣ مهاجمة البيانات:

بعد أن رأينا كيف تتم مهاجمة الخادم، نرى في هذا النوع من الهجوم كيف تتم

مهاجمة البيانات (Data-driven attack)، وهو الهجوم الذي يستهدف البيانات التي تنتقل بواسطة البروتوكول، ولا يستهدف الخادم الذي ينفذ هذا البروتوكول. إما أن يكون هدف الهجوم هو زرع فيروس من خلال رسائل البريد الإلكتروني، أو أن يكون هدف الهجوم هو الحصول على أرقام البطاقات الائتمانية خلال انتقالها عبر الشبكة.

مرة أخرى لا تستطيع جدران الحماية فعل الكثير في هذا المجال، فالبيانات لابد أن تمر، وإلا فكيف يمكن أن تؤدي الشبكة مهمتها، وكيف يمكن أن ينفذ المستخدمون أعمالهم؟ ولكن في بعض الأحوال يستطيع جدار الحماية حجب المعلومات الضارة، فيمكن مثلاً تركيب أحد البرامج الفاحصة للفيروسات (Virus scanners) في جدار الحماية لفحص البريد الإلكتروني وغيره من بروتوكولات نقل الملفات.

ربما كان السلاح الأقوى هنا هو " الوعي "، وذلك بتوعية المستفيدين بما عليهم اتباعه عند جلب الملفات لأجهزتهم أو عند إرسال البريد للآخرين، ومد هؤلاء المستفيدين بالبرمجيات اللازمة لحماية أجهزتهم، بما في ذلك برامج مكافحة الفيروسات أو برامج التشفير.

٥-٢-٤ وسائل العلاج : أساليب التحقق من سلامة الرسائل:

في جميع أنواع الهجوم التي تندرج تحت أسلوب إقحام الرسائل وتزوير المعلومات رأينا أن الحل المثالي يكمن في استخدام أساليب التحقق من سلامة الرسائل، ومنها استخدام المجموع الاختباري (Checksum) والقيمة الاختبارية (Hash)

٥-٢-٤-١ المجموع الاختباري (Checksum):

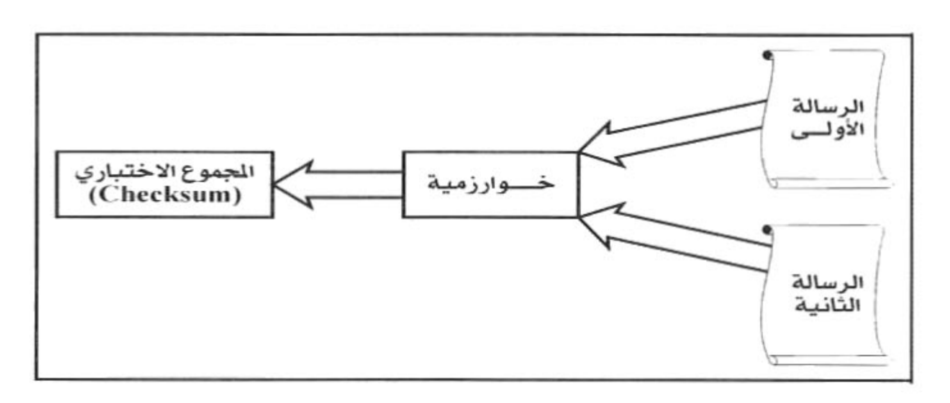
المجموع الاختباري (Checksum) هو عبارة عن رقم يتم احتسابه بناء على مجموعة من البيانات، بهدف اكتشاف أي تغيير قد يطرأ على هذه البيانات، أو أي خطأ قد يحدث خلال نقلها، وهذا الاختبار مفيد للتأكد من أمن قنوات الاتصال. فإذا قام الطرف المرسل بحساب المجموع الاختباري قبل إرسال البيانات، وقام الطرف المستقبل بالشيء نفسه عند استقبال البيانات؛ فإنه يمكن ببساطة مقارنة النتيجتين لمعرفة ما إذا كانت

البيانات المنقولة قد وصلت سليمة، أم أن هناك خطأ قد تم خلال عملية النقل. ويمكن استخدام المجموع الاختباري كذلك للتأكد من سلامة البيانات المخزنة، بحساب هذا المجموع وتخزينه، ثم إعادة احتسابه من وقت لآخر ومقارنته بالنتيجة المخزنة.

يتكون المجموع الاختباري عادة من مجموعة محدودة من الحروف (Bytes)ويحتل مساحة أقل بكثير من المساحة التي تحتلها البيانات الأصلية، ولذلك فمن الناحية النظرية هناك احتمال بأن يعطي المجموع الاختباري نفس النتيجة عند احتسابه لمجموعتين مختلفتين من البيانات، وهو ما يعرف بالتضارب (Collision)، ولكن خوارزميات (Algorithms)المجموع الاختباري قد تم تصميمها بحيث تجعل احتمالات التصادم أقل ما يمكن كما يبدو في الشكل (٥ - ٣).

شكل (٥-٣)

التضارب (Collision) يحدث عندما ينتج نفس المجموع الاختباري من رسالتين مختلفتين



ويختلف تصميم هذه الخوارزميات تبعًا للأخطاء التي يفترض أن تكتشفها هذه الخوارزميات، فبعضها الهدف منه اكتشاف الأخطاء العشوائية غير المتعمدة مثل فقد أجزاء من البيانات، أو اكتشاف مجموعة متجاورة من الحروف التي بها أخطاء، وهذه

تكون عادة الأخطاء الناتجة عن التشويش في خطوط الهاتف التي مازالت تشكل وسيلة النقل الأكثر شيوعًا، وهي تلك الأخطاء التي نسمعها في الهاتف كنوع من الضوضاء أو الشوشرة التي لا تمنعنا في الهاتف من الإلمام بالمقصود من العبارات التي نسمعها، ولكن مع الحاسب فهذا التشويش كاف لإفساد الرسالة بالكامل.

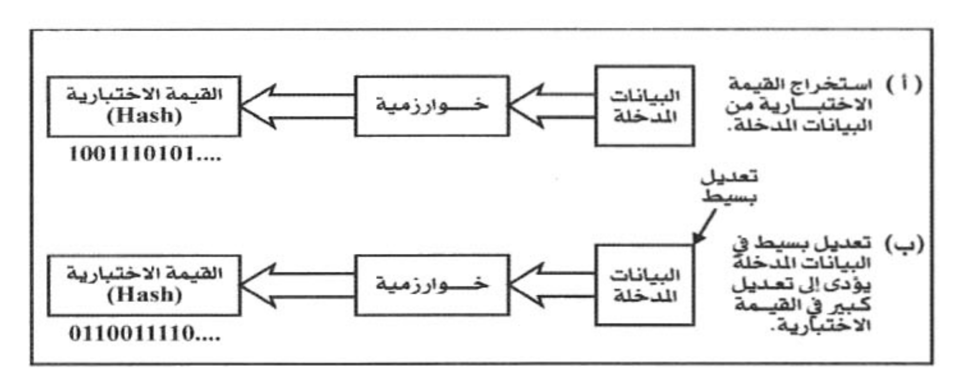
ولكن ماذا لو لم يكن الخطأ عشوائيًا وكان التغيير متعمدًا؟ هل يمكن أن يقوم المهاجم بإجراء تعديل متعمد مع المحافظة على نفس قيمة المجموع الاختباري؟ للأسف هذا صحيح بالنسبة للعديد من خوارزميات المجموع الاختباري لأنها غير مصممة لاكتشاف الأخطاء المتعمدة.

٥-٢-٤-٢ القيمة الاختبارية (Hash):

لعلاج مشكلة الأخطاء المتعمدة التي لا يعالجها المجموع الاختباري يتم استخدام القيمة الاختبارية (Hash)، وفي هذا الأسلوب يتم توليد مجموعة من الحروف (String) ثابتة الطول مستنتجة من مجموعة من الحروف أطول بكثير، وتتميز بأن أي تعديل بسيط في المدخلات (الرسالة الأصلية) يتسبب في تعديل كبير في المخرجات (القيمة الاختبارية) شكل (٥-٤).

شكل (٥-٤)

تعديل بسيط في البيانات المدخلة يؤدي إلى تعديل كبير في القيمة الاختبارية



وهذا الأسلوب لا يستخدم في نفس الأغراض التي يستخدم فيها المجموع الاختباري. وعلى أي حال يجب أن تتوفر الخصائص التالية في خوارزميات القيمة الاختبارية:

(١) يجب إن يكون من المستحيل من الناحية العملية إنشاء مجموعة من البيانات يكون لها نفس القيمة الاختبارية لمجموعة أخرى من البيانات. ويمكن تحقيق ذلك بتصميم الخوارزمية بحيث إنها لا يمكن عكسها، أو تنفيذها بالعكس، لتخرج النص الأصلي من القيمة الاختبارية (أي أن الهندسة العكسية هنا مستحيلة).

(٢) يجب أن يكون طول القيمة الاختبارية (Hash) كبيرًا نسبيًا بما يكفي لمنع المهاجمين من إعداد قائمة من الملفات المصطنعة، واحد لكل قيمة من القيم الاختبارية. وبالتالي يستطيعون استبدال أي رسالة فيحلون محلها الملف الذي ينتج نفس القيمة الاختبارية المقابلة لهذه الرسالة. ومن الناحية العملية فإن القيمة الاختبارية المناسبة يجب ألا يقل طولها عن (١٢٨بت)، بل يفضل أن يكون (١٦٠بت) [Zwicky ٢٠٠٠].

(٣) يجب في حالة إدخال أي تعديل ولو بسيط جدًا في بيانات الرسالة (مدخلات الخوارزمية) فإن القيمة الاختبارية يجب أن تتغير بشكل كبير جدًا. أي أن تعديل "

خانة " (Bit) واحدة في الرسالة يجب أن يتسبب في تعديل نصف حجم القيمة الاختبارية. وهذا الأمر مهم للغاية، لأنه يمنع المهاجم من أن يأخذ في تجربة تغيير كل " خانة " (Bit) في الرسالة واحدة واحدة حتى يصل إلى محاكاة القيمة الاختبارية المقابلة.

تستخدم القيمة الاختبارية في اكتشاف تزوير البيانات، وهي تعتبر الأساس في إعداد " التوقيعات الرقمية " (Digital signatures) التي سنتحدث عنها في الفصل السابع. كما يستخدم هذا الأسلوب كذلك في نظم التحقق من الشخصية (Authentication)، ففي كثير من النظم لا يتم تشفير كلمات السر وإنما يتم إعداد قيمة اختبارية لها بدلاً من التشفير. والسبب هو أن التشفير قابل للكسر، فإذا استطاع المهاجم كسر الشفرة التي تم بها تشفير كلمة السر استطاع الحصول عليها واستخدامها للحصول على ما يشاء من معلومات، مما يجعل تشفير كلمات السر وإرسالها مشفرة عبر الشبكة أمرًا غير مأمون العواقب. ولكننا سبق وأوضحنا أن من شروط (القيمة الاختبارية) هو عدم إمكان تطبيق الهندسة العكسية عليها واستعادة الأصل منها، مما يجعل استخدامها أكثر أمنًا. وعندما يتطلب الأمر التحقق من شخصية المستفيد، يتم استنتاج القيمة الاختبارية من كلمة السر المدخلة ومقارنتها بما هو مخزن في الجهاز، فإذا تطابقتا فإن ذلك يعني أن المستفيد قد أدخل كلمة السر الصحيحة.

هناك حالة واحدة يمكن فيها أن يخترق المهاجم هذا الأسلوب، وهي الحالة التي يقوم فيها المستفيدون بالدخول عن بعد من خلال شبكة الإنترنت، ويتم توليد القيمة الاختبارية في خادم الشبكة المرسلة لكلمة السر، ومن ثم فإن ما يمر في شبكة الإنترنت هو القيمة الاختبارية وليس كلمة السر نفسها. في هذه الحالة يمكن خداع النظام باستخدام القيمة الاختبارية وإرسالها بادعاء صدورها من خادم الشبكة المرسلة. وللتغلب على هذه المشكلة تعمد الشبكات التي تستخدم أساليب قوية للتحقق من الشخصية إلى استخدام قيمة عشوائية يتم تغييرها في كل مرة يتم فيها الدخول إلى

الحاسب تسمى (Nonce). هذه القيمة المتغيرة تتم إضافتها إلى المعلومات التي يتم استنتاج القيمة الاختبارية منها، وذلك قبل إرسال هذه القيمة عبر الشبكة. وتمنع هذه الطريقة أولئك الذين يمارسون التنصت من قراءة القيمة الاختبارية وإعادة استخدامها.

٥-٣ الاقتحام (Intrusion):

الاقتحام (Intrusion) هو أشهر أنواع انتهاك المعلومات وأكثرها انتشارًا، فالمقتحم (Intruder) يستطيع بعد اقتحامه أحد الأجهزة استخدام هذا الجهاز كيفما يشاء وبكامل صلاحيات المستفيد الشرعي صاحب الجهاز. ومن ثم فالمقتحم إذا نجح في الاقتحام فإنه يستطيع ارتكاب جميع أنواع الانتهاك الأخرى كالتنصت أو التزوير أو إقحام الرسائل [Mcclure ١٩٩٩].

٥-٣-١ وسائل الاقتحام:

لدى المهاجمين عشرات الوسائل لتنفيذ اقتحام ناجح لأجهزة الحاسب. تتفاوت هذه الوسائل من الهندسة الاجتماعية [داود ٢٠٠٠ب] (حيث يقوم المهاجم مثلاً بانتحال اسم شخصية مرموقة في الشركة والاتصال بمدير النظام طالبًا منه تغيير كلمة السر فورًا لأداء عمل عاجل)، مرورًا بالتخمين (حيث يقوم المهاجم بتجربة أزواج من الأسماء وكلمات السر حتى ينجح زوج منها في الدخول إلى النظام)، ووصولاً إلى الوسائل الأخرى للدخول التي لا يحتاج فيها المهاجم إلى معرفة أسماء أو كلمات سر. وهنا تساعد جدران الحماية بشكل كبير في منع الاقتحام بهذه الأساليب، فمهمة جدار الحماية هي منع كل محاولات الدخول إلى النظام التي لا تستخدم اسم مستخدم وكلمة السر. وإذا تمت تهيئة جدار الحماية بشكل جيد فإن ذلك سيساعد على الحد من قدرة المهاجمين على الوصول إلى حسابات المستفيدين من خارج الشبكة، والنجاح في اقتحامها بواسطة الهندسة الاجتماعية أو التخمين. أي أن جدار الحماية المعد جيدًا يمكن أن يغطي الوسائل الثلاثة للاقتحام، وبذلك يكون من أفضل وسائل مقاومة

الاقتحام. وحتى عند نجاح المقتحم في اختراق جدار الحماية فسيكون لدى مسئول أمن المعلومات سجل وقائع (Log) يوضح الأسلوب الذي اتبعه المقتحم أو محاولاته للتخمين، ويسهل هذا السجل على مسئول الأمن مهمة تقوية جدار الحماية بمزيد من الاحتياطات.

٥-٣-٢ الاقتحام العشوائي:

التجربة العشوائية لكلمات السر أسلوب يلقى النجاح في كثير من الأحيان، حيث يجرب المقتحم كل القيم الممكنة لمعرفة كلمة السر أو لكسر شفرتها. فقد يقوم المقتحم بتجربة كلمات القاموس مثلاً حتى يصل إلى الكلمة الصحيحة. وتوجد برامج على شبكة الإنترنت لكسر كلمة السر (Password crackers) تقوم بهذه المهمة مثل برنامج *(LΦpht Crack)* من شركة *(L Φpht)*، وهذا البرنامج يستخدم كلمات القاموس والتخمين العشوائي لكسر الشفرة، ويمكن خلال عدد محدود من الساعات الحصول على الكلمة المطلوبة. وبمعرفة أن كلمات السر المشفرة لنظام " وندوز إن تي " يتم حفظها في ملف اسمه (SAM) في الفهرس (\WinNT\system٣٢\config)، فإن البرنامج يقوم بإحدى ثلاث طرق للوصول إلى هذه المعلومات:

(١) استقبال هذه المعلومات (Importing) إذا أمكن تشغيل البرنامج على خادم " إن تي " مباشرة.

(٢) قراءة النسخة الاحتياطية من ملف (SAM) المخزنة على أحد الأشرطة، أو على قرص الطوارئ، أو من فهرس (\WinNT\repair).

(٣) التنصت على النظام والتقاط هذه الكلمات خلال مرورها بالشبكة باستخدام البرنامج المساعد (readsmb.exe).

٥-٣-٣ الأبواب الخلفية:

وجود الأبواب الخلفية في النظم والتطبيقات يسهل عمليات الاقتحام اللاحقة. ومن

هذه الأبواب الخلفية حسابات المستفيدين المخفاة في هذه النظم (Hidden accounts)، وللقارئ أن يتخيل أن لديه " موجه " (Router) عند مدخل الشبكة الداخلية الخاصة به، ويتولى هذا الموجه مهمة حماية الشبكة عن طريق مراقبة حزم الرسائل المارة من وإلى الشبكة، وتخيل وجود حساب مستفيد مخبأ في هذا الموجه وأن لهذا الحساب صلاحيات مطلقة (Administrator-level authorities)، وأن كلمة السر المرافقة لهذا الحساب لا يمكن تغييرها! أي ثغرة أمنية هذه!! وللأسف فهذه الثغرة تكاد تكون موجودة في (معظم) أجهزة الشبكات التي تقتنيها الشركات والمؤسسات وكثير من الجهات الأمنية نفسها ! ففي عام ١٩٩٨ اكتشف أن شركة (٣COM) قد زرعت في محولاتها (Switches) الموجودة في منتجاتها (Core Builder) و(Super Stack II) حساب مستفيد مخفي له صلاحيات كاملة، وكان اسم المستفيد هو (Debug) وكلمة السر هي (Synnet)، و كان هذا الحساب غير قابل للتعديل أو الإلغاء من جانب المستفيد، كما كان غير مرئي وغير موثق ضمن وثائق النظام [Brenton ١٩٩٩]، هذا يعني أن مقتني هذه الأجهزة برغم اتخاذه كل الإجراءات الأمنية إلا أنه معرض للاقتحام من خلال هذا الباب الخلفي.

في معرض دفاعها قالت شركة (٣COM) أنها ليست الشركة الوحيدة التي تفعل ذلك، وأنها إنما فعلت ذلك لتسهيل مهمة الفنيين الذين يقدمون المساعدة الفنية للعميل إذا ما نسي العميل كلمة السر الخاصة بمدير النظام. ومن المنطقي أن تكون هناك بدائل أخرى لمساعدة مدير النظام صاحب الذاكرة الضعيفة، كأن يتم فصل الجهاز عن الشبكة وتشغيل برنامج لاستعادة كلمة السر الضائعة.

وفي الوقت الحالي يصعب أن يتأكد العميل من أن الجهاز الذي يقتنيه من أجهزة الشبكة لا يحتوي على حسابات مخفية. فلابد من اتخاذ احتياطات إضافية، مثل عدم السماح بإصدار أوامر التحكم في أجهزة الشبكة عن بعد، حتى لا يتمكن من يعرف هذه الحسابات من الاستفادة منها [Reynolds ٢٠٠٠].

٥-٣-٤ انتحال الشخصية:

ذكرنا أن من أسهل وسائل الاقتحام هو انتحال شخصية واحد من المستفيدين الشرعيين، وذكرنا من قبل أن أفضل أسلوب لمعالجة كلمات السر ليس التشفير وإنما أسلوب القيمة الاختبارية (Hash) حتى نمنع المقتحم من استخدام كلمة السر المشفرة كما هي، أي دون كسر شفرتها، لخداع النظام. ولكن هذا لن يفيد إذا نجح المقتحم في (تخمين) كلمة السر.

أسلوب آخر يتبعه المقتحم للحصول على كلمة السر عن طريق الاتصال بالمستفيد وإقناعه بأنه هو خادم الموقع ويعرض عليه رسالة مزورة تطلب منه إعادة إدخال الاسم وكلمة السر، فيقدم المستفيد طائعًا مختارًا اسمه وكلمة السر على طبق من ذهب للمقتحم! ولعلاج ذلك يتم تحديد الاتصال بين المستفيد وخادم الموقع من خلال قناة مشفرة، أو أن يكون على الخادم إثبات شخصيته للمستفيد بجملة متفق عليها في كل مرة يصدر رسالة أو أمرًا للمستفيد.

٥-٣-٥ اختطاف المواقع (Site Hijacking):

من خلال هذا النوع من أنواع الاقتحام " اختطاف المواقع "(Site Hijacking) يستطيع المقتحم الاستيلاء على جهاز أو على جلسة اتصال يقوم بها مستخدم انتهى من إثبات شخصيته. ويحدث هذا الاستيلاء في العادة على أحد الأجهزة التي تتصل عن بعد، وأحيانًا يتم الاستيلاء على أحد الأجهزة الواقعة على المسار الذي يصل بين الحاسب البعيد وبين جهاز الحاسب المحلي الذي يعمل عليه المستفيد.

ويمكن الحماية من الاختطاف الذي قد يقع على حاسب بعيد بعدم السماح بالاتصال من جانب الأجهزة البعيدة، إلا تلك التي نثق في أمنها وعدم إمكان الدخول إليها من قبل غير المختصين. ويمكن تحقيق ذلك باستخدام جدار الحماية أو بإعادة تهيئة خادم الشبكة، فمثلاً يمكن تهيئة خادم نقل الملفات (FTP server) بحيث يسمح بقبول دخول مستفيد مجهول (Anonymous) من داخل الشبكة ولكن الدخول من

خارج الشبكة لابد أن يكون من جانب مستفيد معروف.

يمكن تفادي عمليات الاختطاف التي تتم بواسطة جهاز وسيط (على المسار بين الحاسب البعيد والجهاز المحلي) باستخدام قناة مشفرة للاتصال، وبذلك لن يكون في مقدور الجهاز الوسيط إقحام أي حزمة تتضمن إثبات الشخصية، لأن صاحب الجهاز لا يعلم الشفرة المستخدمة ومن ثم فلن تقبل منه هذه الحزمة.

أما اختطاف المواقع على الحاسب البعيد فهو أكثر سهولة، خاصة إذا تعود المستفيد ترك جهازه مفتوحًا. ويمكن التغلب على ذلك بأن يتم، بشكل آلي، إغلاق أي حاسب يظل مفتوحًا دون نشاط لمدة معينة.

٥-٤ اعتراض البث (Session Hijacking):

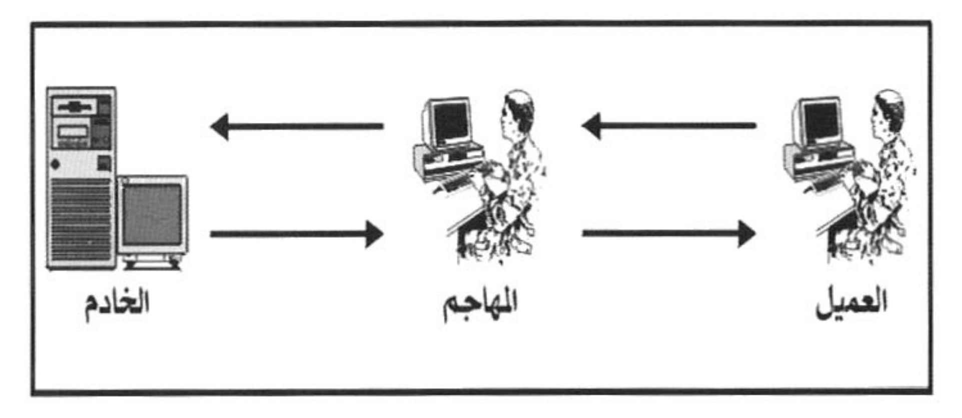
"اعتراض البث" نعني به هذا النوع من الاقتحام الذي يكون فيه المهاجم في مكان ما بين العميل والخادم ويكون مسلحًا بأداة تحليل الحزم (Packet analyzer)، ويطلق على هذا النوع اسم (Man in the middle) وهو نوع من أنواع اختطاف المواقع (Site Hijacking) الذي تم شرحه في القسم ٥-٣-٥ .

وهناك أساليب أخرى لتنفيذ هذا النوع من الهجوم، وهي تستغل كون معظم الشبكات لا تستخدم أساليب قوية لتحديد شخصية المستفيد. وما لم يبادر طرفا الاتصال (العميل والخادم) من حين لآخر بالتأكد من شخصية الطرف الآخر فمن الممكن جدًا أن يجد أحدهما نفسه يتعامل مع مهاجم وليس مع الطرف الذي يظن.

ويعرف " اعتراض البث " (Session hijacking) بأنه تدخل طرف ثالث في الحوار، الشكل (٥-٥). وما يحدث هو أن المهاجم يترقب أن يبدأ أي طرفين اتصالاً مشروعًا. وبعد بدء جلسة الاتصال بينهما يقوم المهاجم بدس بعض الأوامر ضمن الحوار الدائر، منتحلاً شخصية أحد طرفي الحوار. وقد تطورت الأدوات المستخدمة في هذا النوع من الاقتحام لجميع أنواع نظم التشغيل [Zwicky ٢٠٠٠]، فهناك أدوات تسمح لأي مهاجم

باعتراض جلسة اتصال يقوم بها مدير النظام، ومن خلال هذه الجلسة يعطي المهاجم نفسه صلاحيات كاملة، وهو بعد ذلك ليس في حاجة إلى الجلسة أو إلى مدير النظام.

شكل (٥-٥)
اعتراض البث



هناك مثلاً برنامج يسمى (C٢MYAZZ) مخصص لاعتراض جلسات نظام التشغيل " وندوز إن تي " وهو يعمل باستخدام التنصت (Spoofing)، وقد استغل هذا النظام حقيقة أن نظام " وندوز إن تي " يستخدم أسلوبين للتحقق من الشخصية: الأول باستخدام كلمة سر مشفرة، والثاني (LanMan) وهو يستلزم إرسال الاسم وكلمة السر دون تشفير، وكان الهدف من هذا النظام الثاني هو التوافق مع النسخ القديمة من النوافذ. وهكذا كان برنامج (C٢MYAZZ) ينتظر في سكون مترقباً أن يقوم أحد المستفيدين بالدخول إلى النظام، هنا يقوم البرنامج بإرسال رسالة إلى المستفيد تطلب منه إرسال الاسم وكلمة السر دون تشفير وتذكر الرسالة أن السبب هو استخدام نظام (LanMan) بدلاً من النظام المشفر، ويستجيب المستفيد ظنًا منه أن من يحاوره هو خادم الشبكة. وهنا يقوم البرنامج باقتناص الاسم وكلمة المرور ويترك العميل يمارس عمله في هدوء.

عند اكتشاف أداء هذا البرنامج قامت شركة " مايكروسوفت " بإعداد تعديلين في نظام التشغيل. أحدهما يتم تركيبه لدى العملاء والآخر يتم تركيبه على خادم الشبكة (NT server)، وباستخدام هذين التعديلين فإن نظام التشغيل الموجود على جهاز العميل سوف يرفض إرسال الاسم وكلمة السر دون تشفير، وبذلك يحرم المهاجم من سرقة هذه المعلومات، ونظام التشغيل على الخادم من ناحيته لن يقبل أي دخول بدون تشفير.

ويوجد برنامج مشابه يعمل على بيئة (Netware) من شركة " نوفيل "، وهو يسمح باعتراض جلسة مدير النظام واستخدامها في رفع صلاحيات المهاجم كما ذكرنا من قبل. وقد كان رد فعل شركة " نوفيل " هو اتباع أسلوب " بصمة الحزمة " (Packet Signature)، وهو أسلوب للتحقق من الشخصية يسمح لكل من الخادم والعميل بالتحقق من شخصية الآخر أثناء الجلسة، وليس فقط في بدايتها. وعند تلقي الخادم رسالة من العميل يقوم بمضاهاة " البصمة " للتأكد من صحة مصدر الرسالة. ولكن كان عيب هذا النظام أنه لم يكن ينفذ بشكل افتراضي (Default) وإنما كان يتطلب تعمد الطرفين استخدامه، ولذلك فإن أي برنامج يستطيع خداع العميل بأن يرسل له رسالة تفيد أن هذا النظام لا يمكن استخدامه خلال هذه الجلسة وبذلك لا يتم استخدامه ولا يتم مضاهاة البصمة.

٥-٥ عرقلة الخدمة (Denial of Service):

"عرقلة الخدمة " (Denial of Service) هو منع أجهزة الشبكة من العمل، وهو أحد أساليب انتهاك شبكات المعلومات المؤثرة، والتي تؤدي إلى أذى شديد وخسارة كبيرة للشركات التي تتعرض لها، وهو أيضاً نوع من الهجوم لا يستفيد منه القائم به ولا يجني من ورائه أي مكسب.

٥-٥-١ الإغراق بالبيانات:

في أواخر عام ١٩٩٤ تعرض الكاتبان " جوش كويتز " و" ميشيل سلاتالا " لما سمي وقتذاك " قنبلة البريد الإلكتروني " وذلك انتقاماً من مقال كتباه عن مجتمع المهاجمين (Hackers) والذي نشراه في مجلة (Wired) فقد قام شخص ما باختراق شبكة مقدم الخدمة الخاص بالكاتبين وقام بتعديل برامج خادم الشبكة بحيث توقف توصيل البريد الإلكتروني لهما، ثم تم إغراق الشبكة بموجة هائلة من رسائل البريد الإلكتروني حتى لم يعد في إمكان الشبكة استقبال البريد المعتاد، وفي النهاية توقف الاتصال بالإنترنت تماماً. والمثال الآخر لهذا النوع من الهجوم هو " دودة موريس " التي تحدثنا عنها في بداية هذا الفصل وسوف نتعرض لها بالتفصيل في الفصل السادس الخاص بالفيروسات.

يمكن إتمام هذا الانتهاك عن طريق إغراق النظام أو الشبكة بالرسائل أو البرامج أو طلبات المعلومات بحيث يقضي النظام أو الشبكة كل الوقت في محاولة الاستجابة لهذه الرسائل أو الطلبات دون جدوى. ولكن المهاجمين الأكثر حنكة يمكنهم عرقلة الخدمة أو تحويل مسارها أو استبدالها بأخرى. فقد يقومون بتحويل كل الاتصالات الواردة لشبكة معينة إلى شبكة أخرى.

٥-٥-٢ استغلال ثغرات السياسة الأمنية للموقع:

في بعض الأحيان يستغل المهاجمون السياسة الأمنية للموقع وما يوجد بها من ثغرات للتسبب في عرقلة الخدمة، فبعض المواقع تلجأ إلى تحديد عدد محدود من المرات لمحاولات الدخول الفاشلة يتم بعدها عرقلة الخدمة عن العميل الذي تتجاوز محاولاته هذا الحد. هنا يلتقط المهاجمون هذا الخيط ويستغلونه بأن يقوموا آليًا بإجراء هذا العدد من محاولات الدخول الفاشلة نيابة عن جميع المستفيدين بانتحال أسمائهم (بما في ذلك مدير الشبكة) وهنا يحدث " عرقلة الخدمة " إذ يتوقف الجميع عن العمل.

الكثير من هذه الأساليب يعتبر من أسلحة حرب المعلومات وبعضها عند استخدامه

يؤدي إلى شلل كامل لشبكات المعلومات [داود ٢٠٠٣].

سنقصر حديثنا هنا عن " عرقلة الخدمة " الذي يتم بطريق العمد، فقد يحدث توقف للخدمة لأسباب فنية أو بسبب أخطاء بشرية، ومن الصعب تفادي هذا الأمر. ولكن أفضل ما يمكن عمله هو تجهيز أكثر من خادم لتعميم الخدمات المختلفة في الموقع، ويختص كل خادم بتقديم خدمة واحدة، بحيث إذا حدث هجوم على أحد الخوادم وتوقف عن العمل فإن ذلك لا يؤثر على باقي الخدمات المقدمة.

٥-٥-٣ الهجوم التعاوني:

يمكن تتبع مصدر الهجوم والوصول إليه باستخدام وسائل التتبع والتحليل المتاحة، ولكن في معظم الأحيان سيتم الوصول إلى الخادم الذي صدر منه الهجوم، أو الخادم الذي تم استغلاله بواسطة المهاجم لشن الهجوم، أما المهاجم نفسه فمن الصعب الوصول إليه ما لم يكن على درجة كافية من الغباء! فعادة يقوم المهاجم بزرع برنامج الإغراق في العديد من الأجهزة المخترقة، بحيث يمكن التحكم في هذا البرنامج عن بعد. وتتم هذه العملية على مدى أسابيع طويلة قبل موعد الهجوم، ويظل برنامج الإغراق هادئًا على كل هذه الأجهزة المخترقة حتى حلول الوقت المناسب، حيث يتم عن بعد إصدار أوامر الهجوم لكل هذه الأجهزة في وقت واحد، فيتم الهجوم من عدة اتجاهات. هذا بالضبط هو السيناريو الذي تم في حالة " عرقلة الخدمة " التي حدثت في عام ٢٠٠٠م وألحقت أضرارًا كبيرة بمواقع عديدة مثل (Yahoo) و (CNN) وغيرها من المواقع الشهيرة.

يندرج تحت تصنيف " عرقلة الخدمة " أيضًا ما يحدث من جانب المهاجمين من إرسال بعض البيانات التي تسبب توقف بعض الأجهزة عن العمل (Halt) أو إعادة تشغيل هذه الأجهزة (Reboot). وكثيرًا ما يحدث تعاون بين مجموعة من المهاجمين يقومون في توقيت معين بمهاجمة خدمة معينة في موقع معين عن طريق إغراقها بالرسائل أو إغراقها بطلبات خدمة مشروعة.

قد يكون من المستحيل تجنب جميع أنواع عرقلة الخدمة بشكل يضمن تماماً عدم حدوثها، ولكن من المهم أن نؤكد أن هذه الأنواع من الهجوم يمكن تجنبها بإعداد جدار حماية مصمم بشكل جيد بحيث يحجب مثل هذه الاقتحامات.

٥ـ٥ـ٤ شن هجوم عرقلة الخدمة:

عند شن هجوم باستخدام حزم (SYN) خلال عملية " الاتصال الثلاثي المبدئي " (TCP's ٣-way handshake) التي تتم عند استخدام بروتوكول (TCP) والتي شرحناها في الفصل الثاني (قسم ٢ ـ ٢ ـ ٦)، يقوم المهاجمون بإرسال حزمة (SYN) من النظام (أ) إلى النظام (ب) مع التمويه بتحديد عنوان مصدر (Source address) وهمي للنظام (أ). عند تلقي النظام (ب) لهذه الحزمة سيحاول الرد بإرسال حزمة (SYN/ACK) إلى العنوان الوهمي. لو أن العنوان الوهمي كان حقيقيًا لقام بالرد بحزمة (RST) ويرسلها إلى النظام (أ)، ولكن في هذه الحالة فإن النظام (ب) سوف يرسل حزمة (SYN/ACK) إلى العنوان الوهمي ولا يتلقى أبدًا حزمة (RST) من النظام (أ) (وهو النظام الوهمي). وعندئذ يصبح الاتصال في حالة (SYN-RECV) ويأخذ مكانه في قائمة الانتظار لتحقيق الاتصال (Connection queue). والنظام (ب) في هذه الحالة يكون قد التزم بالموافقة على قبول الاتصال، وهكذا يبقى هذا الاتصال المزعوم محتلاً مكانه في قائمة الانتظار إلى أن ينقضي الزمن المفترض لإتمام الاتصال (Connection-establishment timer)، وهذا الزمن يختلف من نظام إلى آخر ولكنه في العادة يتراوح بين ٧٥ ثانية في حده الأدنى إلى ٢٣ دقيقة في بعض النظم [McClure ١٩٩٩]، ولما كانت قائمة الانتظار عادة قصيرة فليس على المهاجم سوى إرسال عدد محدود من حزم (SYN) كل عشر ثوان مثلاً حتى يتعطل هذا المنفذ بالكامل. ولهذا اكتسب هذا الأسلوب من أساليب " عرقلة الخدمة " جاذبية واسعة الانتشار في أوساط المهاجمين، إذ إنه لا يحتاج إلى إمكانيات كثيرة (مادية أو معرفية) لإرسال هذا الفيض من حزم (SYN)، وكذلك لأن استخدام المصدر الوهمي يحمي المهاجم من انكشاف شخصيته.

ويتضمن الفصل التاسع شرحًا واسعًا لحزم نظام TCP/IP

٥-٥-٤-١ الإجراءات المضادة للهجوم:

من أجل اكتشاف ما إذا كان النظام تحت الهجوم في وقت معين يستطيع مدير الشبكة أو مسئول أمن المعلومات إصدار الأمر (netstat)، إذا كان نظام التشغيل يتضمن هذا الأمر، وهو أمر يبين حالة الشبكة في لحظة ما. فإذا اكتشف المسئول وجود عدد كبير من الاتصالات في حالة (SYN-RECV) فهذا مؤشر قوي على تعرض النظام لهجوم باستخدام حزم (SYN). ويمكن اللجوء إلى أحد الإجراءات الأربعة التالية للتقليل من أثر هذا الهجوم:

(١) زيادة حجم قائمة الانتظار، لاستيعاب عدد أكبر من هذه الحزم.

(٢) خفض زمن إتمام الاتصال (Connection-establishment timer) لسرعة التخلص من هذه الحزم وإخراجها من قائمة الانتظار.

(٣) اقتناء بعض البرمجيات التي تساعد على كشف محاولات الانتهاك من هذا النوع، وكثير من نظم تشغيل الشبكات الحديثة تتضمن مثل هذه البرمجيات.

(٤) اقتناء نظام كشف الانتهاك (IDs).

٥-٥-٥ هجوم " قطرة الدمع "(Teardrop Attack):

هناك نوع آخر من أنواع الهجوم أطلق عليه اسم " هجوم قطرة الدمع " (Teardrop Attack)، ولكي نفهم كيفية شن هذا الهجوم علينا أن نفهم دور المعلومات الواردة في مقدمة حزمة الرسائل في إعادة ترتيب الرسالة.

عندما يتسلم " الموجه " (Router) حزمة رسائل أكبر مما ينبغي، فإنه يقوم بتجزئتها قبل تمريرها، وفي هذه الحالة يستخدم الموجه حقلين من حقول مقدمة الرسالة (IP Header) هما حقل " مؤشر التجزئة "(Fragmentation offset field) وحقل " طول الرسالة " (Length Field) لتمكين النظام المتلقي للرسالة من إعادة

ترتيب أجزائها بالشكل الصحيح. وعندما يستقبل النظام المتلقي حقل مؤشر التجزئة وبه القيمة (٠) فإنه يفترض إما أن هذا هو الجزء الأول من الحزمة، أو أن هذه الحزمة لم تتعرض للتجزئة.

عند حدوث التجزئة، يستخدم النظام المتلقي حقل " مؤشر التجزئة " لتحديد مكان هذا الجزء من الرسالة (بعده عن بدايتها)، ويستخدم حقل " طول الرسالة " كنوع من التأكيد للتأكد من أنه لا يوجد خطأ في حساب حقل " مؤشر التجزئة " وأنه لم تحدث أخطاء خلال نقل الرسالة، فمثلا إذا تم نقل الجزء الأول من الرسالة ووضعه في مكانه وتم نقل الجزء الثالث ووضعه في مكانه، ثم أتى الدور على الجزء الثاني من الرسالة ووجد النظام المتلقي أن محتويات حقل " طول الرسالة " تشير إلى أن الجزء الثاني أطول مما كان مقدراً له وأنه سيمتد ليغطي جزءاً من محتويات الحقل الثالث، فلابد وأن خطأ ما قد حدث. عندئذ سيحاول النظام إعادة ترتيب أجزاء الرسالة من جديد، فإذا لم يتمكن فإنه سوف يرسل في طلب إعادة إرسال أجزاء الرسالة مرة أخرى.

والآن كيف يتم هجوم " قطرة الدمع "؟ يقوم المهاجم بإرسال حزمة بيانات عادية بحيث يحتوي حقل " مؤشر التجزئة " فيها على القيمة (٠) وهذا أمر طبيعي، ولكنه يقوم بالتلاعب في بيانات حقلي " مؤشر التجزئة " و" طول الرسالة " في الحزم التالية من الرسالة، وعندما يصل الجزء الثاني من الرسالة (الحزمة الثانية) يقوم النظام المتلقي بمراجعة حقل " مؤشر التجزئة " لمعرفة المكان الذي يضع فيه هذا الجزء من الرسالة، فيكتشف أن هذا الحقل يشير إلى أن هذا الجزء يبدأ قبل انتهاء الجزء الأول، وعندما يراجع النظام الحقل الآخر (حقل " طول الرسالة ") يكتشف أن طول هذا الجزء أقل من أن يمتد بعد نهاية الجزء الأول، أي أن الجزء الثاني سيكون متضمناً بالكامل في الجزء الأول. وهذا الخطأ ليس في الحسبان، فالنظام إذا اكتشف أن الجزء الثاني من الرسالة يمتد بعد الجزء الأول (Overlap) فإنه قد يطلب إعادة الإرسال، ولكن في هذه الحالة فإن هذا النوع من الخطأ لا يوجد له برنامج للتعامل معه(Handling Routine) ومن ثم، وفي الكثير من الأحيان، يتوقف النظام المتلقي تماماً عن العمل.

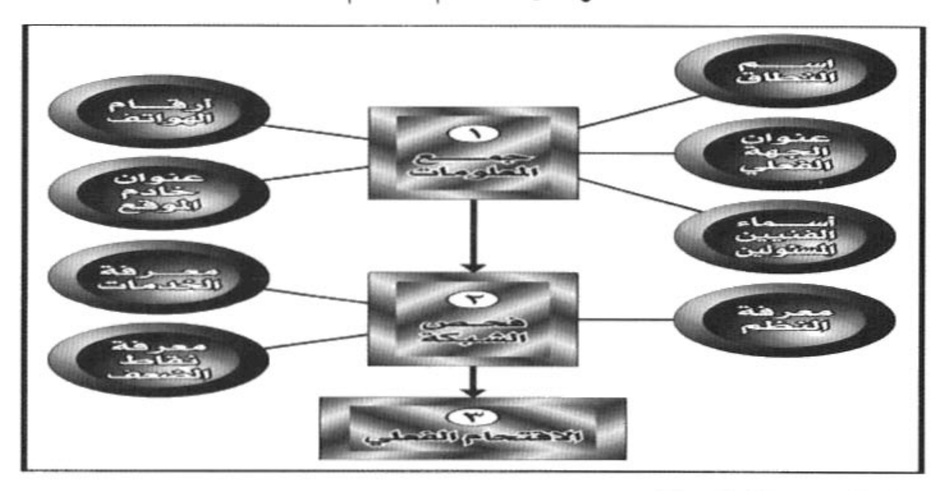
٥-٦ سيناريو عملية اقتحام ناجحة:

سنقدم فيما يلي السيناريو الكامل الذي يوضح العمليات التي يقوم بها المهاجم لاقتحام أحد المواقع، ونحن نوردها هنا ليس لتوجيه المهاجمين لكيفية تنفيذ الهجوم ولكن لتنبيه مسئولي أمن المعلومات في الجهات المختلفة عما ينبغي عليهم القيام به، وعن كيفية تفسير ما قد يلاحظونه من إشارات قد تمر مرور الكرام.

تمر عملية الاقتحام بعدة مراحل لابد منها لكي يتم الاقتحام بنجاح، وهي مرحلة جمع المعلومات عن الشبكة، ثم مرحلة فحص الشبكة لمعرفة النظم التي تعمل فيها، ومعرفة الخدمات التي يتم تقديمها من خلال المنافذ المختلفة على هذه النظم، والتعرف على الثغرات الأمنية أو نقاط الضعف الموجودة بالشبكة. وثالثة هذه المراحل هي مرحلة الاقتحام الفعلي التي استعرضنا مختلف أنواعها فيما سبق من هذا الفصل. الشكل (٥ - ٦) يبين هذه المراحل.

شكل (٥-٦)

مراحل اقتحام النظام



٥-٦-١ جمع المعلومات:

يبدأ المهاجم بجمع المعلومات اللازمة عن موقع الضحية، ولنفترض أنه لا يعرف حتى

اسم الموقع. يستطيع المهاجم استغلال أحد الأوامر عظيمة الفائدة لمستخدمي شبكة الإنترنت وهو أمر (Whois) فيقوم بتوجيهه لقاعدة البيانات العامة في (InterNIC) والتي تضم كافة المواقع المسجلة على شبكة الإنترنت. فيمكن السؤال مثلاً عن موقع " معهد الإدارة العامة " بتوجيه السؤال التالي: (Whois IPA) ويأتي الرد بسرد عدة مواقع تشترك مع معهد الإدارة العامة في الاختصار IPA. ومن بينها نجد اسم الموقع (ipa.edu.sa) والذي يبدو الأقرب لما نريده. وهنا نستطيع جمع كم أكبر من المعلومات بالسؤال عن هذا الموقع بالتحديد (Whois ipa.edu.sa) فتأتي معلومات أكثر مثل اسم النطاق وعنوان الجهة وأسماء الأشخاص الفنيين المسئولين عن الموقع، وأرقام هواتفهم وفاكساتهم وعنوان بريدهم الإلكتروني، وعنوان خادم الموقع. ولنحاول أن نستعرض فائدة كل معلومة من هذه المعلومات الثمينة، وكيفية الاستفادة منها في الاقتحام:

(١) **اسم النطاق** (Domain Name): سوف يستخدم في جمع المزيد من المعلومات فكل موقع فرعي (كفروع المعهد) وكل مستفيد من موظفي أو طلاب معهد الإدارة العامة سيقع ضمن هذا النطاق.

(٢) **عنوان الجهة الفعلي**: ربما أتاح هذا العنوان للمهاجم الدخول إلى الموقع بحجة تقديم طلب عمل أو طلب التحاق بالمعهد، ومن ثم ربما يتاح له الدخول على أحد الأجهزة الموجودة بالمعهد في قاعات الدراسة أو الأجهزة المخصصة لجمهور المتعاملين. وهذه الأجهزة تسهل عليه الأمور كثيرًا، فالاختراق من الداخل أكثر سهولة لأنه لا يمر بجدران الحماية! ومن هذه الأجهزة قد يستطيع المهاجم التعرف على بعض أسماء العاملين وأرقام هواتفهم.

(٣) **أسماء الفنيين المسئولين**: هذه المعلومة مفيدة جدًا عند استخدام " الهندسة الاجتماعية " في الهجوم، كأن يطلب أحد المستفيدين في الهاتف ويقول له: أنا " أحمد الراشد " من مركز الحاسب الآلي وقد كلفني الأستاذ " مازن القرشي " بالاتصال بك لأن هناك مشكلة في اسم المستفيد الخاص بك على أحد أجهزة الخدمة لأننا اكتشفنا أنك قد غيرت كلمة السر أثناء إعداد النسخة الاحتياطية

للنظام مما سبب عدم التوافق في المعلومات المخزنة على جهاز الخدمة، فما هو اسمك المسجل في الحاسب؟ وما هي آخر كلمة مرور أدخلتها؟. ربما نجحت هذه الوسيلة في مد المهاجم باسم مستفيد وكلمة سر صحيحة. حتى لو كانت صلاحيات هذا المستفيد محدودة إلا أن هذا يشكل له مكان قدم كافيًا يمكن أن يؤدي في النهاية إلى الحصول على صلاحيات كاملة على النظام.

(٤) **أرقام الهواتف:** معظم أرقام هواتف موظفي المعهد تبدأ بالرقم (٤٧٤) ويتلوه أربعة أرقام. وعند طلب هذا الرقم يتم الاتصال مباشرة بالموظف صاحب الرقم دون الحاجة إلى المرور بموظف السنترال. وبالتالي يستطيع المهاجم توقع كافة أرقام الهواتف في المعهد بتجربة بعض الأرقام القريبة من الرقم الموجود ضمن المعلومات التي تم الحصول عليها، مما يمكنه من الوصول إلى بعض المستفيدين بالأسلوب الذي ذكرناه آنفًا (أسلوب الهندسة الاجتماعية). أو يستطيع المهاجم القيام بشن محاولات اتصال متعددة بشكل آلي باستخدام (War Dialer) وهو برنامج يقوم بالاتصال بمجموعة كبيرة من أرقام الهاتف، وبهذه الوسيلة يستطيع المهاجم اكتشاف أي من هذه الأرقام متصل بجهاز حاسب، وهكذا يستطيع المهاجم بعد الحصول على اسم مستفيد وكلمة سر استخدامهم مع هذا الرقم في الدخول مباشرة من الخارج إلى شبكة معهد الإدارة العامة.

(٥) **عنوان خادم الموقع:** لنا أن نتوقع أن هذا العنوان على الأقل يقع ضمن نفس النطاق المخصص لشبكة معهد الإدارة العامة على الإنترنت. ولكن المهاجم لا يعرف حتى هذه اللحظة هل هذا العنوان يقع قبل جدار الحماية أو بعده؟

الآن يستطيع المهاجم جمع المزيد من المعلومات عن عناوين الإنترنت (IP addresses) باستخدام الأمر (nslookup) الذي سيعطيه عنوان خادم الموقع بدقة، ومن ثم يستطيع المهاجم العثور على أكثر من عنوان خادم داخل الموقع مما يسهل له عملية مهاجمتهم في وقت واحد إن أراد شل عمل الموقع [Brenton ١٩٩٩] فمن بين المعلومات التي سيحصل عليها المهاجم من استفساراته عنوان خادم البريد الإلكتروني، والخادم المخصص لخدمة

نقل الملفات، مما سيفيده في توجيه هجومه للهدف المحدد بالضبط. فهو الآن في موقف يجعله قادرًا على إغراق خادم الملفات بطلبات الملفات، أو إغراق خادم البريد بالرسائل الوهمية، أو اختراق خدمة البريد الإلكتروني نفسها للاطلاع على هذه الرسائل وتزويرها إن أراد.

محركات البحث (Search engines) هي أيضًا يمكن أن تكون مصدرًا مهمًا للبيانات يحصل منه المهاجمون على بيانات قيمة عن الشبكات الداخلية للشركات. بالاستفسار عن (IPA) من موقع(Google.com)، الذي يستضيف أقوى محركات البحث على الإنترنت على الإطلاق، يستطيع المهاجم الحصول على الكثير من المعلومات المفيدة مثل عنوان خادم البريد الإلكتروني، ونظام التشغيل المستخدم ونسخته، وعنوان الشبكة الفرعية التي يوجد بها خادم البريد(IP subnet)، وغير ذلك من المعلومات.

٥-٦-٢ فحص الشبكة:

من المهم فحص الشبكة لمعرفة موقع جدار الحماية، ومعرفة الخدمات المقدمة، ورسم خارطة كاملة للموقع. ويمكن استخدام أمر (Tracerout) لتتبع الشبكة من خادم لآخر، وأحيانًا يختصر هذا الأمر ليصبح (Tracert) هذا الأمر يظهر اسم وعنوان كل " موجه " في الشبكة، وهي الموجهات التي سيتعين على المهاجم المرور بها والتعامل معها عند اقتحامه للشبكة.

وتفيد معرفة الخدمات المقدمة في معرفة المنافذ (Ports) المتاحة على الشبكة، كما يفيد فحص الشبكة في معرفة أي نظام من النظم يكون من السهل مهاجمته. وهنا يلزم اتباع الخطوات التالية، علمًا بأنه توجد بعض الأدوات الجاهزة التي تقوم بتنفيذها:

١- معرفة كل النظم الموجودة على الشبكة.

٢- معرفة الخدمات المقدمة على كل من هذه النظم.

٣- معرفة كل نقاط الضعف الموجودة في كل من هذه الخدمات.

٥-٦-٢-١ معرفة النظم:

يمكن استخدام (Ping scanner) وهو يشكل إحدى الوظائف المتوفرة ضمن برنامج (AG NetTools) من شركة (AG) ويقوم (Ping scanner) بإرسال طلب (ICMP) لكل عنوان (IP address) على الشبكة وينتظر الرد. فإذا تلقى ردًا فمعنى ذلك أن هذا العنوان فيه موقع نشط (Active host) باستخدام هذا الأسلوب يقوم البرنامج بإعداد قائمة بالمواقع النشطة، كما يحاول ترجمة عناوين الشبكة (IP addresses) إلى اسم الموقع المصاحب لها. ويستخدم هذا البرنامج من خلال واجهة رسومية متقدمة.

٥-٦-٢-٢ معرفة الخدمات:

يمكن استخدام برنامج (AG NetTools) كذلك لمعرفة المنافذ (Ports) النشطة، ومن ثم الخدمات المقدمة على الموقع. ويتم ذلك عن طريق اختبار المنافذ على الموقع الضحية واحدًا واحدًا لاكتشاف النشط منها. تمامًا مثلما يقوم لص السيارات بالمرور على صف السيارات المنتظرة في موقف السيارات ويجرب مقابض الأبواب حتى يعثر على سيارة ينفتح بابها.

ومن واقع الخدمات التي يظهر أنها نشطة يمكن استنتاج نوع نظام التشغيل المستخدم. ولكن تعاني هذه الوسيلة من بعض القصور، وأهم مظاهر هذا القصور هو أن هذه المحاولات لاختبار المنافذ سوف يتم تسجيلها بواسطة الموقع الضحية مما ينبه مسئول الموقع أن هناك هجومًا يتم التحضير له. والعيب الثاني هو أن معظم جدران الحماية (Firewalls) ومصافي الحزم (Packet filters) تستطيع كشف هذا الأسلوب ومنعه، لأن هذه العملية تعتمد على إرسال حزمة الاختبار، والتي تتضمن مقدمتها في حقل العلامات (Flag field)[١] علامة (SYN=١) التي تطلب بدء جلسة اتصال (Communication session)، بينما يجب أن يتم هذا الطلب من جانب أحد الأجهزة داخل الشبكة وليس من خارجها. وهكذا تستطيع مصفاة الحزم أن تحجب هذا الأمر.

---

(١) سنتحدث بالتفصيل في الفصل التاسع عن حقل العلامات ومحتوياته.

ولكي يتغلب المهاجمون على تسجيل الموقع لمحاولاتهم فإنهم يلجأون إلى الفحص بأسلوب (TCP half scanning) حيث لا يتم اتصال كامل مع الموقع، وإنما يتم فقط إرسال حزمة بدء الاتصال التي تحتوي على العلامة (SYN=١) فإذا استجاب النظام فمعنى ذلك أن هذا المنفذ نشط ويقدم الخدمة المخصصة له. وهنا يقوم برنامج الاقتحام فورًا بإرسال حزمة تحتوي مقدمتها على العلامة (RST=١) التي تعني إعادة الوضع إلى ما كان عليه سابقًا، فيتم معرفة وضع المنفذ دون أن يتم تسجيل ذلك في سجل الوقائع (Log) لأن الاتصال لم يكتمل.

ولكن ذلك لا يحل مشكلة مصافي الحزم التي لا تقبل حزمة تأتي من خارج الشبكة وتحتوي مقدمتها على العلامة (SYN=١)، ويمكن حل هذه المشكلة باللجوء إلى أسلوب (FIN scanning) حيث يتم تجنب إرسال العلامة (SYN=١) لبدء الاتصال. وبدلاً من ذلك يتم إرسال حزمة بها العلامتين (FIN=١ , ACK=١)معًا حيث تشير العلامة (ACK=١) إلى الموافقة على بدء جلسة الاتصال (وكأنما قد سبق إرسال طلب بدء الاتصال من النظام رغم أن ذلك لم يحدث) والعلامة (FIN=١) تشير إلى إنهاء جلسة الاتصال والهدف منها تفادي تسجيل الواقعة في سجل الوقائع (Log). في هذه الحالة إذا استجاب النظام بحزمة تحتوي مقدمتها على العلامتين (RST=١, ACK=١) فيعني ذلك أن هذا المنفذ خامل ولا يقدم الخدمة المتوقعة، وإذا تجاهل النظام هذه الرسالة ولم يرد عليها فمعنى ذلك أن هذا المنفذ نشط ويقدم الخدمة. وبذلك يمكن التوصل إلى المنافذ النشطة وحصرها على النظام. وللأسف فهذا الأسلوب لا تستطيع معظم جدران الحماية أو مصافي الحزم الاستاتيكية التصدي له (سنقدم شرحًا وافيًا لمصافي الحزم الاستاتيكة والديناميكية وجدران الحماية وحقل العلامات Flag field في الفصل التاسع المخصص لجدران الحماية).

٥-٦-٢-٣ معرفة نقاط الضعف:

بعد أن تمكن المهاجم من معرفة كل النظم الموجودة على الشبكة وتعرف على

الخدمات التي يتم استخدامها على كل نظام من هذه النظم، عليه الآن أن يبحث عن نقاط الضعف التي يمكن أن يستغلها. ويمكن الوصول إلى نتائج مرضية عن طريق التجربة والخطأ، ولكن هذا (التخبط) قد ينبه القائمين على أمر الشبكة، أما المهاجم المتمرس فيدرس الموقف أولاً بعناية ويعرف أين تكمن مواطن الضعف ومواطن القوة ولا يلجأ إلى التجربة والخطأ.

ويمكن اللجوء إلى الأسلوب اليدوي لاكتشاف نقاط الضعف من خلال خدمة الدخول عن بعد (Telnet) للاتصال بخدمات أخرى. هذه الخدمات عادة ما تعرف نفسها بوضوح للمتصلين عن بعد، وذلك بهدف تسهيل عملية البحث عن الأخطاء (Troubleshooting)، ولكن المهاجمين يستغلون هذه الوسيلة للحصول على المعلومات.

فإذا وجه المهاجم أمر (Telnet) التالي من سطر الأوامر:

telnet mailsys.ipa.edu.sa ٢٥

فمعنى ذلك أنه يطلب بدء جلسة اتصال (Telnet) مع منفذ (SMTP) على خادم البريد (mailsys.ipa.edu.sa) بينما يحدد الرقم (٢٥) رقم المنفذ المطلوب إقامة جلسة الاتصال معه، وهو منفذ (SMTP)، وذلك بدلاً من المنفذ الافتراضي لخدمة (Telnet) وهو المنفذ رقم (٢٣).

وهكذا سيرد خادم البريد بأنه يستخدم (Microsoft exchange mail service) مثلاً، مما يعني أن نظام التشغيل هو(Windows NT)، وسيرد كذلك بأن نسخة النظام هي ٥,٠ (مثلاً)، كما سيبين رقم التركيب (Build number) الذي يبين تركيب أي برامج تصحيحية (Service packs) على هذه النسخة. هذه المعلومات التي تطوع بها النظام بمجرد خداعه بالاتصال بمنفذ (SMTP) باستخدام خدمة مخصصة لمنفذ آخر (Telnet) تفيد كثيرًا في معرفة نقاط الضعف الموجودة في نسخة نظام التشغيل المبينة. إذ إن المهاجم سيبدأ في البحث عن نقاط الضعف في نظام التشغيل هذا، وفي هذه النسخة بالذات.

ويستطيع المهاجم استخدام عدد من الأوامر من خلال الاتصال بالمنافذ المختلفة على النحو المبين في الجدول التالي [Brenton ١٩٩٩].

جدول رقم (٥-١)

الأوامر التي يمكن استخدامها من المنافذ المختلفة عند الدخول باستخدام خدمة (Telnat)

الخدمة	المنفذ	الأوامر	ملاحظات
FTP	٢١	**user, pass, stat, quit**	يمكن استخدام هذا المنفذ لتنفيذ الأوامر فقط، وليس لنقل الملفات.
SMTP	٢٥	**helo, mail from:, rcpt to:, data, quit**	يمكن تزوير رسائل البريد الإلكتروني باستخدام هذه الأوامر.
HTTP	٨٠	**get**	لن يتم تنفيذ الأمر، ولكن المهاجم سوف يعرف أن الخدمة قائمة على هذا المنفذ.
POP٣	١١٠	**user, pass, stat, list, retr, quit**	يمكن الاطلاع على البريد الإلكتروني من خلال الاتصال بمنفذ POP٣
IMAP	١٤٣	**login, capability, examine, expunge, logout**	يمكن استخدام هذا المنفذ للدخول أو الخروج.

هذا الأسلوب اليدوي في اكتشاف الثغرات ونقاط الضعف قد يستغرق بعض الوقت لتحقيق الهدف، ولذلك يلجأ الكثير من المهاجمين إلى الأسلوب الآلي لاكتشاف الثغرات. ويتم ذلك باستخدام برنامج يقوم آليًا بتنفيذ كل خطوات الفحص والاستكشاف، كما يمكن للبرامج الآلية عمل هذا الفحص لمجموعة كاملة من النظم، وفي النهاية يخرج البرنامج للمستخدم قائمة من الثغرات التي يمكن استغلالها. وكمثال على ذلك برنامج (Asmodeus security scanner) من شركة (Web trends)، يقوم هذا البرنامج بتحديد النظم النشطة الموجودة في الشبكة، ثم يبدأ البرنامج في البحث عن المنافذ ويقدم تقريرًا عن الثغرات التي يجدها. ولا يعني خلو التقرير من الثغرات عدم وجود

هذه الثغرات، بل لابد من المزيد من البحث لتحديد هذه الثغرات، سواء كان هذا التحديد يتم من جانب المهاجمين، أو من جانب مسئولي أمن الشبكات. إذ ربما احتاج الأمر إلى تجربة شن هجوم معين لاكتشاف إذا ما كان هذا الهجوم لديه فرصة النجاح أم لا.

استعرضنا في هذا الفصل العديد من أساليب انتهاك شبكات المعلومات والتي تشكل الخطر الحقيقي الذي يجب أن يلتفت إليه الجميع. فمهاجمي اليوم ربما كان بعضهم من الهواة.. ولكن مهاجم المستقبل سيكون مجرمًا محترفًا أو عضوًا في شبكات الجريمة المنظمة.

ولا نود أن نختم هذا الفصل عن انتهاك شبكات المعلومات دون أن نحذر من بعض خبراء أمن المعلومات الذين يرتزقون من تشغيل برامج الكشف عن نقاط الضعف في الشبكات المختلفة ويعرضون للبيع التقارير المخرجة التي يتلهف عليها المهاجمون، ولذلك فعلى الشركات والجهاز الحكومي توخي الحذر من الاستعانة بمثل هؤلاء لفحص أمن شبكاتهم.

الفصل السادس
الفيروسات

بعد أن تعرضنا فى الفصل السابق للأساليب المختلفة التي يستخدمها المهاجمون لانتهاك شبكات المعلومات، كان من الضروري أن نتحدث عن خطر داهم يهدد هذه الشبكات. لذلك فإن هذا الفصل خصصناه للحديث عن الفيروسات، أخطر ما يهدد أمن شبكات المعلومات. فنبدأ الفصل بتعريف الفيروسات وشرح العوامل التي تؤدي إلى انتشارها. ثم نستعرض أنواع الفيروسات المختلفة كالفيروس، ودودة الحاسب، وحصان طروادة، والبرامج الهجومية (جافا وآكتف إكس). ثم نستعرض هذه الأنواع، فندرس الفيروس من خلال خصائصه الثلاث: التضاعف والتخفي وإلحاق الأذى بنظم الحاسب، وندرس دودة الحاسب وأشهر أنواعها، ثم نتحدث عن " حصان طروادة " كواحد من أنواع الفيروسات الخطيرة. ننتقل بعد ذلك إلى الأساليب المختلفة لحماية الشبكات من الفيروسات، وبرامج مكافحة الفيروسات ومواصفاتها. ثم نختم الفصل بالحديث عن التوقعات لمستقبل الفيروسات.

٦ـ١ ما هي الفيروسات؟

من المؤكد أن أكثر جرائم الحاسب إمعانًا في الشر هي جريمة نشر الفيروسات، فمن ينشر الفيروس ينشره وهو لا يدري من سيصيب؟ وماذا سيدمر؟ وما هو حجم الأضرار التي ستصيب الضحايا؟ أي أنها جرائم من مستوى الجرائم التي ترتكب بواسطة أسلحة الدمار الشامل، النووية والكيماوية، مع الفارق بالطبع [داود ٢٠٠٠أ].

من المؤكد أيضًا أن الفيروسات قد وجدت بيئة رائعة للانتشار بعد ظهور شبكة الإنترنت.. وسطًا رائعًا للانتشار، وكأنك منحت الأسماك بحيرة من الماء ترتع فيها وتتكاثر. فمن كان يحلم من صانعي الفيروسات بمثل هذه الوسيلة السهلة والمضمونة لنشر فيروسه في أكبر عدد ممكن من الأجهزة وفي أقل مدة زمنية. وقد أصبحت الفيروسات الآن خطرًا حقيقيًا يهدد الاقتصاد والحكومات والأفراد [Parker ١٩٩٨] [Abrams ١٩٩٨] [Elliot ٢٠٠٠].

٦-١-١ تعريف الفيروس:

على مدى العقود الثلاثة الماضية ثار جدل طويل بين خبراء أمن المعلومات حول الاتفاق على تعريف محدد لفيروس المعلومات، وكان هناك خلط كبير لدى العامة بينه وبين " دودة الحاسب "(Worm)، و" حصان طروادة " (Trojan horse) [Parker ١٩٩٨] وأصبح التمييز بين هذه الأنواع ينفرد به المتخصصون، فيعرف البعض الفيروس بأنه " أي برنامج، أو مجموعة من التعليمات، التي تلحق ضرراً بنظام المعلومات أو بالبيانات، على أن تكون لديه القدرة على التضاعف والانتشار " [داود ٢٠٠٠ ب] [Hyatt ٢٠٠١].

وذكر " ماكجرو " و" موريست " في تقريرهما إلى مجلس بحوث أمن المعلومات الأمريكي [McGraw ٢٠٠٠] (IRC) أن الفيروس هو " أجزاء من برامج ذات أهداف شريرة يتم إلحاقها ببرامج أخرى وتنتشر عند تنفيذ البرنامج الملوث ". والبرامج ذات الأهداف الشريرة (Malicious code) يعني بها أي برامج تضاف أو تحذف أو تعدل في أحد نظم المعلومات بهدف إلحاق الأذى بالنظام أو تعديل مهامه.

أما إذا أردنا تعريفًا للفيروسات يلقى قبولاً من الجميع فهو أن الفيروس: " برنامج له ثلاث خواص: التضاعف، التخفي، إلحاق الأذى " وأول من توصل إلى هذه الصيغة التوافقية هو " كريس برينتون " [Brenton ١٩٩٩] ووافقه في ذلك آخرون [Bently ٢٠٠٠] [Ghosh ٢٠٠١].

٦-١-٢ عوامل انتشار الفيروسات:

هناك العديد من العوامل التي تقف وراء الانتشار الكبير للفيروسات في هذه الأيام. هذه العوامل لخصها تقرير " ماكجرو " [McGraw ٢٠٠٠] الذي قدمه إلى مجلس بحوث أمن المعلومات في الولايات المتحدة، فيما يلي:

(١) **انتشار الشبكات:** بازدياد ارتباط الحاسبات ببعضها من خلال شبكة الإنترنت ازدادت سهولة شن الهجمات، كما ازداد عدد هذه الهجمات تبعًا لذلك. وأصبح من النادر اليوم أن نرى جهاز حاسب غير مرتبط بشبكة الإنترنت، ويدعم ذلك

الاتجاه ما نشهده من الاعتماد المتزايد لدى الأفراد والشركات على البريد الإلكتروني وصفحات النسيج كوسيلة اتصال وتواصل. وباختصار شديد فإن مهاجم اليوم لا يحتاج إلى الوصول المباشر إلى جهاز الحاسب لزرع فيروسه.

كما ساعد انتشار الشبكات على شن أنواع آلية من الهجوم لا يتدخل فيها البشر. وقد حدث في فبراير عام ٢٠٠٠م هجوم تسبب في عرقلة الخدمة في العديد من مواقع التجارة الإلكترونية، وكان السبب في نجاح هذا الهجوم هو ما سبقه من اختراق لعدد من أجهزة الحاسب الكبيرة التي استخدمت خلال هذا الهجوم في إغراق مواقع التجارة الإلكترونية بطلبات وهمية. واستمرار انتشار الشبكات يعني المزيد من حالات الهجوم، والمزيد من الضحايا، والمزيد من الخطر.

(٢) **زيادة تعقيد النظم:** بازدياد حجم نظم المعلومات الحالية ودرجة تعقيدها، زاد اعتمادها على نظم التشغيل في توفير الحماية الأمنية لها. ونظم التشغيل نفسها تضم آلاف البرامج التي تحتوي على عشرات الملايين من أوامر البرمجة، وفي نظم بهذا الحجم لا يمكن تفادي الثغرات. وزاد من تفاقم المشكلة استخدام لغات لا تتمتع بالحماية الأمنية (مثل لغة C ولغة C^{++}) التي لا تقاوم أبسط أنواع الهجوم مثل " إغراق المساحات الوسيطة بالبيانات " (Buffer overflow).

ولو افترضنا جدلاً أننا استخدمنا نظم تشغيل آمنة تماماً ولغات آمنة تماماً وبرامج تطبيقية لا تقل أمنًا، فإن تركيب هذه المجموعة كلها معًا على أجهزة الخدمة، والذي يتم أحيانًا بواسطة مستخدم غير متخصص أو ليس لديه الوعي الأمني، تركيب هذه البرامج بشكل غير سليم قد يفتح ثغرات كبيرة تنفذ منها الفيروسات وغيرها.

من جهة أخرى، فإن التطبيقات الضخمة المعقدة تشكل بيئة صالحة لاختباء الفيروسات فلا يلحظ وجودها أحد. فقد نستطيع فحص برنامج صغير وتأكيد نظافته وخلوه من الفيروسات، ولكن من المستحيل عمل ذلك في تطبيقات اليوم التي تملأ حاسباتنا الشخصية، ناهيك عن التطبيقات الضخمة التي تعمل في الشركات والبنوك والدوائر الحكومية.

(٣) **سهولة الإضافة إلى النظم:** تفخر الكثير من نظم المعلومات اليوم بأنها نظم قابلة للتوسع (Extensible systems) بمعنى أنها تقبل التحديث والإضافة سواء من جانب المورد أو المستخدم أو من جانب أطراف ثالثة، وتأتى هذه الإضافات في شكل برامج منقولة (Mobile code) فالبرامج التي تستعرض الإنترنت (Web brow-sers) يسهل الإضافة إلى إمكانياتها بإنزال بعض البرامج من شبكة الإنترنت، وتحذو حذوها الكثير من نظم التشغيل وبرامج معالجة الكلمات والبريد الإلكتروني وغيرها. وفي عالم الأعمال اليوم يتم اقتناء البرامج من جانب الشركات بدرجة كبيرة من التسرع للمحافظة على القدرة التنافسية للشركة وإحرازها قصب السبق (في تطوير وتحسين شكل موقعها على الإنترنت، أو فيما تقدمه من خدمات مباشرة لعملائها)، ولذلك فمعظم (إن لم يكن جميع) البرمجيات ونظم التشغيل الحالية تجدها قابلة للتوسع مما يسهل إقحام الفيروسات. وأوضح مثال على ذلك هو الكيفية التي انتشر بها فيروس " ميليسا " (Melissa virus)حيث استغل قابلية برنامج البريد الإلكتروني " أوت لوك " (Outlook) للتوسع. فقد تم كتابة الفيروس في صورة (Script)تحتويه رسالة بريئة للغاية انخدع بها معظم المستخدمين، وعند فتح هذه الرسالة يتم تنفيذ الفيروس الذي يقوم بالحصول على عناوين البريد الإلكتروني من القائمة التي يحتفظ بها مستخدم الجهاز لمن يتصل بهم، ثم يرسل الفيروس نسخًا من الرسالة (نسخًا من نفسه) إلى هذه العناوين. وبأسلوب مشابه عملت " جرثومة الحب " (Love bug) الشيء نفسه وانتشرت الانتشار نفسه.

٦ـ٢ أنواع الفيروسات:

تنقسم الفيروسات التقليدية إلى عدة أنواع: الفيروس(Virus)، والدودة (Worm) وحصان طروادة (Trojan horse) وبرامج الهجوم (Attack scripts)، وقد أضيفت لها مؤخرًا بعض الأنواع الحديثة من الفيروسات وهي برامج " جافا " الهجومية (Java attack applets) وبرامج " أكتف إكس " (Active X controls) وفيما يلي تعريف كل من هذه الأنواع:

١- **الفيروس (Virus):** هو جزء من برنامج ذو أهداف شريرة يتم إلحاقه ببرامج الحاسب الآلي، وعند تنفيذ البرنامج الملوث يبدأ انتشار الفيروس.

٢- **الدودة (Worm)**: وهو نوع خاص يصيب الحاسبات المرتبطة بشبكات الحاسب الآلي، وبدلاً من أن ترتبط ببرامج الحاسب الآلي فإن الدودة تشن هجومًا مدبرًا للانتقال من جهاز إلى جهاز آخر عبر الشبكة.

٣- **حصان طروادة (Trojan horse):** وهو يشبه الفيروس في أنه يخفي أهدافًا شريرة في أحد برامج الحاسب الآلي والتي تبدو كأنها أهداف نبيلة، كأن يتخفى البرنامج الذي يسرق كلمات السر في هيئة برنامج تسجيل الدخول (Logins) ولو أنه لا يعتبر نوعًا من أنواع الفيروسات.

٤- **برامج الهجوم (Attack scripts):** وهي برامج قام بكتابتها محترفون بحيث تستفيد من الثغرات الأمنية ونقاط الضعف الموجودة في شبكات المعلومات من أجل شن هجوم على أجهزة الحاسب في الشبكة. تقوم معظم هذه البرامج بتدمير قوائم الانتظار للخدمات المختلفة عن طريق إغراق المساحات الوسيطة بالبيانات.

٥- **برامج جافا الهجومية (Java attack applets):** هي برامج مخفاة في صفحات النسيج (Web pages)، وهي تنشط عند تشغيل مستعرض الصفحات (Web browser).

٦- **برامج أكتف إكس (Dangerous Active X controls):** وهي تلك الأجزاء من البرامج التي تسمح للتعليمات غير البريئة في برامج التطبيقات بالتحكم في هذه التطبيقات.

هذا التصنيف لأنواع الفيروسات يتغير باستمرار فتقترب الأنواع من بعضها وتتشابه وتظهر أنوا ع جديدة، ويبين الجدول (٦-١) بعض الأمثلة الحية على أخطر أنواع الفيروسات التي ظهرت في تاريخ شبكات الحاسب الآلي [McGraw ٢٠٠٠].

جدول (٦-١)
بعض أخطر الفيروسات عبر التاريخ

الفيروس	السنة	التصنيف	وصف الفيروس
الشفرة الحمراء Code Red	٢٠٠١	دودة	ضربت شبكة الإنترنت في أغسطس ٢٠٠١م وأحدثت الكثير من الخسائر.
جرثومة الحب Love bug	٢٠٠٠	برامج منقولة (فيروس)	أسرع الفيروسات انتشارًا عبر التاريخ، وكان مكتوبًا بلغة (VB script) واستغل برنامج البريد الإلكتروني " أوت لوك (Outlook) للانتشار. وقدرت خسائره بمبلغ ١٠ بلايين دولار.
برنامج Trinoo	٢٠٠٠	برنامج الهجوم عن بعد (Attack script)	أشهر أنواع هجوم عرقلة الخدمة (Denial of service) ووقع في فبراير ٢٠٠٠ وانتشر عن طريق زرع برامج عن بعد.
فيروس مليسا	١٩٩٩	برامج منقولة (فيروس)	ثاني أسرع الفيروسات انتشارًا عبر التاريخ واستخدم في انتشاره البريد الإلكتروني، وقد أصاب أكثر من ١,٢ مليون جهاز حاسب خلال ساعات قليلة.
دودة Explore.zip	١٩٩٩	برامج منقولة (دودة)	دودة تنتقل عبر البريد الإلكتروني استغلت بعض الثغرات الأمنية في نظام النوافذ (Microsoft windows) للانتشار.
فيروس Happy ٩٩	١٩٩٩	فيروس	واسع الانتشار أصاب الحاسبات الشخصية.
فيروس CIH	١٩٩٨	فيروس	شديد الخطورة، ويهاجم (Bios) في أجهزة الحاسب الشخصي وقد انتشر بسرعة هائلة في آسيا قبل اكتشافه.
الثغرة الخلفية Back orifice	١٩٩٨	برنامج هجومي	برنامج تم تركيبه بواسطة المهاجمين عن طريق التحكم من بعد في الأجهزة التي تعمل في بيئة النوافذ.
برامج هجومية Attack Scripts		برنامج هجومي	برامج موجودة على شبكة الإنترنت أعدها خبراء ويتداولها المهاجمون ويستخدمونها في مهاجمة أهدافهم. واسعة الانتشار وتقوم عادة بإغراق المساحات الوسيطة بالبيانات (Buffer overflow)
أكتف إكس	١٩٩٧	برامج منقولة	أنشأت هذه النوعية من البرامج عند ظهورها وضعًا أمنيًا خطيرًا بسبب الاعتماد على فطنة المستخدم وحدها لعدم الوقوع في شراكها.
برامج جافاالهجومية	من ١٩٩٦ إلى ١٩٩٩	برامج منقولة	برامج موجودة على بعض المواقع في شبكة الإنترنت استفادت من الثغرات الأمنية الموجودة في لغة " جافا ". تم رصد ١٧ هجومًا كبيرًا من هذا النوع.
دودة موريس	١٩٨٨	دودة	دمر هذا البرنامج ٦٠٠٠ جهاز حاسب (حوالي ١٠٪ من الإنترنت في ذلك الوقت).
مترجم طومسون	١٩٨٤	حصان طروادة	تم زرعه في مترجم لغة " C" لينتشر في أي برنامج تتم ترجمته.

أما أخطر الفيروسات المنتشرة حالياً في أجهزة الحاسب فيمكن الحصول عليها من موقع شركات مكافحة الفيروسات على شبكة الإنترنت [Symantec ٢٠٠٣]، وسنقدم فيما يلي شرحاً تفصيلياً لطبيعة ومهمة الأنواع المختلفة من الفيروسات، وسنركز على أهمها.

٦-٢-١ الفيروس (Virus):

هو أول وأخطر أنواع الفيروسات، وهو صاحب الاسم الأصلي، وذكرنا من قبل أن تعريف الفيروس هو أنه برنامج يتميز بخواص ثلاث: التضاعف، والتخفي، وإلحاق الأذى. وسنحاول فيما يلي أن نشرح طبيعة الفيروس من خلال هذه الخواص الثلاث.

٦-٢-١-١ التضاعف:

لابد لكل فيروس من وسيلة للتضاعف أو التكاثر بهدف الانتشار. والفيروس لا يستطيع الانتشار بمجرد التواجد على القرص الصلب، بل لابد للملف الملوث الذي دخل إليه الفيروس وأصبح جزءاً منه أن يصل إلى ذاكرة الحاسب وأن يبدأ تنفيذه. هذا هو الشرط لكي يصبح الفيروس نشطاً ويمكنه أداء مهامه. والتنفيذ هنا إما أن يكون مباشراً بقيام المعالج (CPU) بتنفيذ البرنامج، أو يكون غير مباشر إذا كان الملف الملوث هو مثلاً وثيقة من وثائق (M.S. Word) يتم عرضها، ومن ثم يلزم تنفيذ الجزء الملوث بها بواسطة برنامج (Word) وهو ما يكون عادة (Macro) ضمن الوثيقة يتولى البرنامج تنفيذه.

ويتم التكاثر عند التحاق الفيروس بأحد الملفات، أو في بعض الأحيان تتم إصابة الملفات التي تحتوي برامج بلغة المصدر، وعندما تتم ترجمتها يحدث المطلوب وهو الوصول إلى المعالج. عند إصابة ملف يتم في العادة وضع جزء صغير من الأوامر في بداية الملف، وتعمل هذه الأوامر على تحميل الفيروس في الذاكرة، أما باقي الفيروس فيبقى في نهاية الملف أو في وسطه.

بوصول الفيروس إلى الذاكرة فإنه يستخدم أحد أسلوبين للتضاعف، فهو إما أن ينتظر تحميل برامج أخرى إلى جواره في الذاكرة فيقوم بالانتقال إليها، وهذا الأسلوب قادر على اختراق كل النظم، حتى النظم ذات الذاكرة المحمية مثل " وندوز إن تي "، مثلما فعل فيروس (Cabanas). وهناك أسلوب آخر وهو أن يختار الفيروس بعض الملفات على القرص الصلب وينتقل إليها مباشرة دون انتظار تحميلها في الذاكرة.

وهناك أيضًا ما يسمى" بالفيروس المصاحب "(Companion virus)الذي يستفيد من أسلوب نظم التشغيل في البحث عن البرنامج المطلوب تشغيله. فعند طلب تشغيل برنامج باسم (Myprog) مثلاً، يقوم النظام أولاً بالبحث عن ملف (Myprog.com) فإن لم يجده يبحث عن ملف (Myprog.exe) وهكذا. يعطي المهاجم لفيروسه الذي يريد مهاجمة البرنامج (Myprog.exe) اسم (Myprog.com) وعند مناداة البرنامج (Myprog) يقوم نظام التشغيل بتنفيذ الفيروس (Myprog.com) الذي يقوم بتحميل البرنامج المطلوب (Myprog.exe) ويبقيان معًا بالذاكرة.

وقد يلجأ الفيروس إلى التوغل في منطقة بدء التشغيل (Boot sector) وهو هنا لن ينتظر تشغيل أي برامج بل عند وصول الفيروس إلى منطقة بدء التشغيل فإنه ينقل أوامر النظام الموجودة بها إلى مكان آخر على القرص ويضع أوامره هو بدلاً منها. وعند بدء تشغيل النظام يتم تشغيل أوامر الفيروس بدلاً من أوامر بدء النظام، وهنا يضع الفيروس نفسه في الذاكرة ثم يشير إلى المكان الجديد الذي نقل إليه أوامر النظام فيتم تشغيل النظام، مع فارق وحيد وهو أن الفيروس الآن يصبح مقيمًا بالذاكرة!

يعمد صانعو الفيروسات إلى وضع بصمة معينة (Signature) في بداية برنامج الفيروس حتى يستطيعون التعرف على الفيروس لتجنب أن يقوم الفيروس بتلويث نفسه مما يعطله عن أداء مهمته. هذه البصمة نفسها يستغلها صانعو برامج مكافحة الفيروسات بالبحث عنها واكتشاف الفيروسات! وفي حالات نادرة نرى الفيروس (ينتحر) عندما يكتشف الفيروس أنه قد تلوث بالفعل بفيروس آخر وأن ذلك ربما أدى إلى كشفه. هنا ينتحر الفيروس ويوقف المهمة!

٦-٢-١-٢ التخفي:

ككل اللصوص لابد للفيروس من التخفي حتى لا ينكشف أمره، ولكي يتخفى الفيروس فإنه يلجأ إلى عدة أساليب:

(١) **البصمة الصغيرة:** كلما كان حجم الفيروس صغيراً (أقل من٢ KB) زادت فرص اختبائه بنجاح في الذاكرة وزادت فرص اختفائه ضمن ملف آخر دون أن يلفت الانتباه، ولضمان صغر الحجم يتم كتابة معظم الفيروسات بلغة التجميع. بل إن بعض الفيروسات مثل " فيروس الفجوة " (Cavity virus) تبحث في الملف عن المساحات الخالية(Null)، أو البيانات المتكررة، بنفس أسلوب برامج ضغط الملفات (File compression)، فيحتل الفيروس هذه المساحات حتى لا يتغير حجم الملف الملوث عن حجمه الأصلي.

(٢) **التلاعب بخصائص الملف:** إذا وجد الفيروس أن الملف الضحية قد تم تحديد خواصه بأنه للقراءة فقط؛ فإن الفيروس يغير هذه الخاصية حتى يسمح لنفسه بتعديل الملف وبعد التعديل يعيد الوضع إلى ما كان عليه. وتصطدم الفيروسات بحائط الصلاحيات في بيئة الشبكات حيث يتطلب الأمر صلاحيات مدير النظام لتعديل خصائص الملفات، وهنا يتمنى الفيروس أن يجد طريقه إلى جهاز مدير النظام!

تعمد الفيروسات كذلك إلى منع تغيير تاريخ تعديل الملف لخداع المستخدم فيظن أن ملفه لم يتم تعديله مؤخراً، ولكن فاحصات الفيروسات (Virus scanners) لا تنخدع بهذه الحيلة.

(٣) **استبدال الرسائل الواردة للنظام:** يستطيع الفيروس إخفاء ما قام به من تعديلات على الملف الضحية. فعند تحميل الفيروس في الذاكرة يبدأ في مراقبة اتصال النظام بالملفات ومساحات الذاكرة، ويستبدل الردود الواردة منها للنظام فيضع بدلاً منها الردود التي يتوقعها النظام لخداعه فيظن أن هذه الملفات غير ملوثة. ويمكن كذلك خداع النظام بعرض ردود غير صحيحة على أوامر استعراض

المحتويات (DIR, MEM) لإخفاء وجوده.

(٤) **إجراءات مضادة لبرامج مكافحة الفيروسات:** تقوم بعض الفيروسات بمراقبة أي بادرة لعملية فحص الفيروسات (Virus scan). وفي هذه الحالة ومن أجل إخفاء هويتها عن هذه البرامج، تقوم بإيهام النظام بوجود فيروس آخر من نوع مختلف، ليقوم النظام بمحاولة القضاء على هذا الفيروس المزعوم (Clean)، وقد تسبب هذه المحاولة انهيار النظام لعدم وجود هذا الفيروس. ولا ينسى الفيروس الحقيقي أن يضع نفسه ضمن قائمة الملفات، بحيث يجد هذا الفيروس نفسه في صورة شرعية عند إعادة تشغيل النظام. ولا يفسد هذه المحاولة إلا إعادة تشغيل النظام (Boot) من قرص سليم نظيف. وجدير بالذكر أن بعض الفيروسات تلجأ لحيلة خبيثة، بالتعرف على عملية ضغط المفاتيح الثلاثة (Ctrl+Alt+Del) وعند حدوث عملية الضغط هذه يقوم الفيروس بتمثيل حالة إعادة تشغيل وهمية لإيهام المستفيد بأن الجهاز تجري إعادة تشغيله، بينما يظل الفيروس قابعًا في الذاكرة.

(٥) **التشفير:** بتشفير بصمة الفيروس يصبح الأمر أكثر صعوبة بالنسبة لبرامج مكافحة الفيروسات، ولكن الأمر لا يصل إلى درجة الاستحالة لأن أساليب التشفير غالبًا ما تكون بسيطة وتستخدم نفس مفتاح التشفير لجميع أوامر برنامج الفيروس. وبمجرد كسر الشفرة التي يستخدمها الفيروس في معامل شركة مكافحة الفيروسات فإنه يمكن إعداد التطعيم اللازم أو العلاج اللازم من آثار الإصابة بالفيروس. وحتى إذا لم يمكن فك الشفرة، فيمكن استخدام البصمة المشفرة كما هي للتعرف على الفيروس.

(٦) " **الفيروس متعدد الأوجه** ": هذا الفيروس (Polymorphic virus) لديه القدرة على تغيير بصمته كلما هاجم أحد الملفات، وهنا تكمن خطورته إذ إن معظم فاحصات الفيروسات (Virus scanners) تعتمد في تعقبها للفيروس على بصمته المعروفة. ويقوم صانعو الفيروس متعدد الأوجه باستخدام مجموعة من أساليب التشفير، وفي كل مرة يهاجم الفيروس أحد الملفات يتم استخدام أحد هذه الأساليب. أي أن على

فاحص الفيروس معرفة هذه الأساليب كلها مسبقًا حتى يستطيع اكتشاف هذا الفيروس. ويصبح الأمر في إطار الاستحالة إذا كان الفيروس يستخدم مفتاحًا عشوائيًا للتشفير.

٦-٢-١-٣ إلحاق الأذى:

بعد أن تتمكن الفيروسات من التكاثر والتخفي، فالخطوة التالية هي انتظار اللحظة المناسبة للهجوم. وهذه اللحظة قد تأتي في صورة حلول تاريخ معين، أو إصابة عدد معين من الملفات، أو حدوث واقعة معينة يترقب الفيروس حدوثها لينشط. ويتراوح الأذى الذي يسببه الفيروس بين مجرد عزف لحن ينطلق من سماعات الحاسب، أو أن يكون مدمرًا فيمسح كل المعلومات المخزنة على القرص الصلب. ويساعد الفيروسات كثيرًا على إلحاق الأذى بنظم الحاسب ضعف الناحية الأمنية في نظم التشغيل التي تفترض أن جميع البرامج التي تنفذها برامج جيدة موثوقًا بها، فتسمح لها بالبقاء في الذاكرة وباستخدام كل ملفات النظام وقوائم الانتظار.

هناك أحد الفيروسات الشهيرة صمم بحيث يقوم بدوره التخريبي فورًا، ففي أبريل ١٩٩٧ وقع الكثيرون ضحايا لأحد هذه الأنواع الذي اشتهر باسم (AOL٤Free.com)، وزاد من انتشاره ظن الضحايا من صياغة الاسم أنه سوف يمنحهم حسابًا مجانيًا في خدمة (AOL)، بينما كان ما تلقوه عبر البريد الإلكتروني ما هو إلا وسيلة ناجحة لحذف جميع ملفاتهم من على القرص الصلب!

ما نود أن نؤكده هنا هو كذب الإشاعات التي تدعي أن الفيروسات قادرة على تخريب الجهاز بحيث لا يصلح للاستخدام أو أنها قادرة على التسبب في احتراق دوائر التشغيل. فلا يمكن للفيروس تخريب أي من مكونات الجهاز، بل أقصى ما يمكن أن يحدث هو تخريب الملفات أو حذفها ودفع المستخدم إلى إعادة تهيئة القرص الصلب. وهذا في بعض الأحيان يشكل في حد ذاته ضررًا بالغًا لبعض الجهات.

٦-٢-٢ الدودة (Worm):

دودة الكمبيوتر هي برنامج من برامج الحاسب، وأحيانًا تكون تطبيقًا كاملاً، وهي تستطيع التكاثر عبر الاتصال بشبكة الحاسب. وبعكس الفيروس، الذي يزرع نفسه في القرص الصلب أو يلتصق بأحد الملفات، فإن الدودة هي برنامج يستطيع الاعتماد على نفسه، فالدودة عادة تحتفظ بنسخة منها فقط في ذاكرة الحاسب، دون أن تحتاج إلى التواجد على القرص الصلب. وهناك منها نوعان:

- الأول يعمل كأحد التطبيقات على جهاز حاسب واحد، ولا تستخدم الدودة الشبكة في هذه الحالة إلا كقناة اتصال تمتطيها للانتقال إلى نظم أخرى.
- أما النوع الثاني فيستخدم الشبكة كجهاز عصبي، أي أنك قد تجد أجزاء من هذه الدودة نشطة على أجهزة حاسب متعددة ويؤدي كل جزء دوره على الجهاز الذي أصابه، وفي بعض الأحيان يكون هناك رأس مدبرة (الجزء المركزي للدودة) تدير عمل باقي الأجزاء، وفي هذه الحالة، ولأنها تبدو كرأس تقود العديد من الأذرع، فيطلق عليها اسم " الأخطبوط "(Octopus)

ولقد ضربت نماذج كثيرة من هذه الدودة شبكات الحاسب حول العالم، ونورد فيما يلي بعض هذه النماذج.

٦-٢-٢-١ الدودة مصاصة الدماء:

يعتبر بعض الدود خبيثًا وبعضه حميدًا، وقد استخدمت شركة " زيروكس " في أوائل الثمانينيات دودة حميدة أسمتها " الدودة مصاصة الدماء "(vampire worm) وكانت هذه الدودة تظل خامدة طول النهار عندما يكون استخدام النظام في ساعات الذروة. وفي الليل تستيقظ الدودة وتنشط وتستخدم المعالج(CPU)، بعد أن يكون هذا المعالج قد تخفف من عبء العمل، لأداء بعض المهام المعقدة والتي تحتاج إلى قدرات المعالج باستمرار(CPU- bound programs).

٦-٢-٢-٢ دودة الإنترنت الهائلة:

لم يكن الاهتمام الموجه لهذا النوع من الفيروسات كبيرًا حتى يوم ٣ نوفمبر ١٩٨٨م عندما أطلقت " دودة الإنترنت الهائلة " (Great internet worm) لتغزو شبكة الإنترنت، ففي أقل من ست ساعات استطاع هذا البرنامج الذي لم يتعد حجمه ٩٩ سطرًا أن يشل كل الأجهزة المرتبطة بالإنترنت من نوع " صن " ومن نوع " فاكس " وعددها ٦,٠٠٠ جهاز. كانت هذه الدودة عندما تصيب أحد الحاسبات تقوم بتشغيل برنامج بسيط في خلفية الجهاز المصاب، ولم يشعر أحد بهذا الأمر في البداية، لولا خطأ بسيط وقع فيه مبرمج الدودة وهو أن الدودة لم تكن تختبر الجهاز قبل إصابته لترى إذا ما كان مصابًا بالفعل أم لا! وكان من أثر ذلك أنه حدثت حالات كثيرة من تعدد الإصابة، التي وصلت في بعض الأحيان إلى مئات المرات، أي أن الدودة تلتحق بالبرنامج عدة مئات من المرات. وبينما كان تشغيل برنامج واحد بسيط في الخلفية أمرًا غير ملحوظ فإن تشغيل عشرات أو مئات البرامج كان لابد أن يعرقل تمامًا عمل الجهاز المصاب. وتفاقمت المشكلة التي سببتها الدودة بسبب اعتمادها في الانتشار على البريد الإلكتروني، فكلما قام مستخدمو الأجهزة بتنظيف أجهزتهم وإعادتها إلى العمل أصيبت من جديد، مما اضطر الكثير من المواقع في ذلك الوقت إلى فصل نظمها عن الإنترنت.

٦-٢-٢-٣ الدودة النووية:

ظهرت في أكتوبر من عام ١٩٨٩ دودة عرفت باسم " الدودة النووية " (WANK) أو (Worms Against Nuclear Killers)، وقد تخصصت هذه الدودة في مهاجمة أجهزة (DEC) فقط. وبرغم أن هذه الدودة كانت من أسوأ الأنواع إلا أنها لم يكن لها أي علاقة بأي نشاط نووي، ولكن الدودة كانت تفعل كلاً مما يأتي:

- ترسل بريدًا إلكترونيًا (ربما لصانع الدودة) به معلومات عن الجهاز المصاب وأسماء المستخدمين وكلمات السر المستخدمة.
- تقوم بتغيير كلمات السر في الأجهزة المصابة.

- تقوم بإنشاء ثغرة خلفية في النظام تمكن من مهاجمته فيما بعد.
- تقوم باستخدام أرقام الهواتف المخزنة في النظام والاتصال بها بشكل عشوائي.
- تصيب ملفات (com) لتتمكن من العودة إلى النشاط بعد إزالتها من الجهاز المصاب.
- تغير من الإعلانات التي تظهر في الموقع المصاب لتعلن عن احتلالها لهذا الموقع.
- تقوم بإخفاء ملفات المستخدم بحيث يخيل له أن كل الملفات قد تم حذفها.

٦-٢-٢-٤ أنواع أخرى من دودة الحاسب:

هناك أنواع أخرى من دودة الحاسب مثل " دودة المحادثة " (IRC worm)والتي تنتقل إلى الجهاز المصاب بمجرد اتصال صاحبه بإحدى قنوات المحادثة (IRC)، وتنتظر في هدوء حتى يصدر إليها أمر، في صورة كلمة معينة، من أحد المشاركين في المحادثة، وكل كلمة لها مدلول معين، وتسبب تنفيذ إجراء معين من جانب الدودة. فهناك كلمة مخصصة لمستخدمي نظام " يونكس " تقوم الدودة عند تلقيها بإرسال نسخة من ملف كلمات السر إلى المتصل الذي أصدر هذا الأمر، وهناك كلمة أخرى مخصصة لمستخدمي نظام النوافذ لحمله على إرسال نسخة من ملف تسجيل البرامج (Registry)، وهناك كلمة ثالثة تمنح المتصل صلاحيات دخول كاملة على النظام وعلى محتويات الأقراص الصلبة فيه.

٦-٢-٣ حصان طروادة (Trojan horse):

حصان طروادة (Trojan horse) هو أحد أساليب الهجوم الخطيرة التي تشبه الفيروسات والتي تخفي مفاجأة شريرة تظهر في وقت معين، ويطلق عليه اسم (Trojan) للاختصار. وهو يختلف عن الفيروس في أنه لا يتكاثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته ويحمل بين طياته توقيت وأسلوب استيقاظه وبدئه النشاط. وهناك العديد من هذه الأنواع تهاجم نظم " يونكس " فتحل محل بعض

تطبيقات الشبكة، فقد تحل محل تطبيق خدمة الاتصال من بعد (Telnet)بحيث يقوم الفيروس عند التعامل مع هذه الخدمة بتسجيل كل الأسماء التي تتصل عن بعد وكلمات السر الخاصة بها. ويستطيع المهاجم استخدام هذه المعلومات فيما بعد ضد هذا النظام أو ضد نظم أخرى منتحلاً اسم إحدى الشخصيات التي قام بتسجيل بياناتها.

وضرب أحد هذه الأنواع مؤخرًا النظم الذي تستخدم " وندوز إن تي " و" وندوز ٢٠٠٠" من خلال شبكة خطوط المراقمة (Dial-up)، وقد تمت برمجته وإخفاؤه ضمن مجموعة من البرامج المساعدة المفيدة التي تغري المستفيدين بإنزالها من شبكة الإنترنت، وعندما يتم إنزال البرنامج يقوم هذا البرنامج المهاجم (Trojan) باستخدام عدد من أوامر (API) لإرسال معلومات عن اسم صاحب الجهاز وكلمة السر الخاصة به للمبرمج الذي قام بإعداد هذا الفيروس. ومن ثم يستطيع هذا المهاجم استخدام هذا الاسم لانتحال شخصية الضحية والدخول إلى مواقع بشبكة الإنترنت مستخدمًا هذه الشخصية.

من بين بعض هذه الأنواع (Trojans) برامج قامت بكتابتها بعض شركات البرمجيات الكبرى. فعند دخول أحد المستفيدين إلى شبكة شركة " مايكروسوفت " يقوم البرنامج بعمل حصر شامل لكل مكونات النظام الخاص بهذا المستفيد من عتاد (Hardware) وبرمجيات(Software)، وعند اتصال الضحية بشبكة الإنترنت يتم إرسال هذه المعلومات إلى شركة مايكروسوفت [Brenton ١٩٩٩] فتحصل الشركة بذلك على بعض المعلومات المفيدة تسويقيًا، كما تستطيع الشركة التأكد من حصول المستفيدين على برامجهم بطريقة مشروعة. وبرغم أن الشركة أكدت أنها تستخدم هذه المعلومات بهدف الدعم الفني فقط، إلا أن الكثيرين اعتبروا هذا نوعاً من الغزو لخصوصياتهم. وليس بعيدًا عن هذه الواقعة ما حدث في مايو ١٩٩٨م عندما أعلن أن شركة (٣ COM) وعدد آخر من منتجي أجهزة الشبكات قد وضعوا ضمن أجهزة المحولات (Switches) والموجهات (Routers) التي ينتجونها نوعًا من ثغرات " الباب الخلفي " (Back door) في شكل حساب (Account) يمكّن من الدخول ولا يمكن

اكتشافه من جانب مستخدم الجهاز، ولا يمكن حذفه أو تعطيله. وادعت هذه الشركة أنها إنما صنعت هذه الأبواب الخلفية بهدف الدعم الفني (لاستخدامها إذا نسي مدير الشبكة كلمة السر الخاصة به)! وحتى إن صح ذلك فإن الشبكة تصبح معرضة أمنياً بشكل جدي.

هناك قصة أخرى نشرتها إحدى كبريات الصحف العربية عن أجهزة اتصال متطورة للغاية حصلت عليها إحدى الدول العربية الكبرى من دولة عظمى، وعند فحص جهاز مخابرات الدولة العربية لهذه الأجهزة تبين أن بها هذا النوع من الفيروسات (Trojan) والذي أعد خصيصاً للحصول على معلومات عن استخدام هذا الجهاز وعن الترددات التي استخدمت عليه، ثم يقوم الجهاز بالاستجابة لإشارة تصل إليه في توقيت معين ليبث ما به من معلومات، ويمكن التقاط هذه المعلومات المبثوثة عن بعد.. بواسطة من؟ ولصالح من؟ .. غير معروف. هذه الأجهزة كانت هدية من الدولة العظمى للدولة العربية الكبرى ضمن المعونة العسكرية التي تقدمها لها. وعند اكتشاف ذلك قامت الدولة العربية بتغليف هذه الأجهزة وأعادت شحنها إلى الدولة العظمى مع بطاقة اعتذار (رقيقة) عن عدم قبول هذه (الهدية). واترك لفطنة القارئ ملء الفراغات بين السطور.

فهل نعتبر هذه التصرفات نوعاً من حصان طروادة (Trojan) أم نوعاً من " الدعم الفني "؟! أو " المعونة العسكرية "؟ أو " الصداقة الدولية "؟!

٦-٣ حماية الشبكات من الفيروسات:

الآن وقد أصبحت عملية كتابة الفيروس وزرعه عملية سهلة، وأصبح العمل على إخفائه ونشره في مساحات كبيرة يتم بسرعة هائلة بالاستفادة من التقنيات المتقدمة للشبكات. مع هذه المستجدات أخذ موضوع حماية الشبكات من الفيروسات حظه الوافر من الاهتمام. ولكننا نعلم جيداً أن الوسيلة الوحيدة المضمونة للتأكد من خلو برنامج ما من الفيروسات هي فحص تعليمات البرنامج بواسطة مبرمج محترف. ولما كانت معظم التطبيقات تمر عبر الشبكة في صورتها القابلة للتنفيذ (Executable code) فليس من

المعقول استخدام الهندسة العكسية على جميع الملفات بالنظام لإعادتها إلى صورتها القابلة للفحص (بلغة المصدر)، ومن ثم فحصها للتأكد من سلامتها! معنى ذلك أنه لا توجد وسيلة عملية لكشف الفيروسات تكون مضمونة بنسبة ١٠٠٪، ولكن هناك وسائل وتقنيات متعددة يمكن استخدام إحداها، أو استخدام مجموعة منها، وهي على النحو التالي:

٦-٣-١ صلاحيات الاستخدام:

من الوسائل الهامة لمكافحة الفيروسات اتباع سياسة محكمة لصلاحيات الاستخدام (Access control). على أن تحدد هذه الصلاحيات لكل مستخدم ما يمكن الوصول إليه من ملفات أو قواعد بيانات، فإن أفضل ما يناسب انتشار الفيروس هو أن يوجد في جهاز يتمتع صاحبه بصلاحيات كبيرة في استخدام الملفات.

٦-٣-٢ حقول المراجعة الرقمية:

يمكن إجراء مراجعة حسابية لبيانات الملفات (Checksum) أو (Cyclic redundancy check) بحيث يمكن تمثيل محتويات الملف بقيمة رقمية. فإذا تغيرت محتويات بايت واحدة في الملف فإن هذه القيمة الرقمية تتغير، حتى لو ظل حجم الملف كما هو. ويمكن من آن لآخر تنفيذ هذه المراجعة للتأكد من عدم حدوث تغيير في الملفات الموجودة على القرص الصلب. وهذا الأسلوب، برغم أنه ليس الأنسب لمكافحة الفيروسات، إلا أنه ناجح في اكتشاف حصان طروادة إذا حاول الحلول محل أحد البرامج.

٦-٣-٣ مراقبة الأداء:

بمراقبة أداء النظام يمكن اكتشاف أي نشاط غريب يتم على النظام. وفي الوقت الحالي يوجد في (Bios) الخاص بجميع أجهزة الحاسب الشخصي نظام لمكافحة

الفيروسات. عند تشغيل الحاسب يقوم هذا النظام بمتابعة كل محاولات الكتابة على السجل الرئيسي لبدء التشغيل (Master boot record). فإذا حاول أحد الفيروسات المتخصصة في مهاجمة قطاع بدء التشغيل (Boot sector) تخزين نفسه في هذه المنطقة فسيتم منعه من ذلك وإخطار المستفيد لطلب موافقته أولاً.

ولكن يعيب هذا الأسلوب أن البرامج العادية (البريئة) كثيرًا ما تتصرف بنفس أسلوب الفيروسات بحيث يصعب التمييز بين الطيب والخبيث. فأمر (FDISK)مثلاً عند تنفيذه سيحسبه (Bios) فيروسًا ويحاول إيقافه. والعيب الثاني في هذا الأسلوب هو الحاجة المستمرة للتدخل البشري والمراقبة للحاسب، وهو أمر لا يمكن الركون إليه باستمرار.

٦-٢-٤ فاحصات الفيروسات (Virus scanners):

تستخدم البرامج الفاحصة للفيروسات " فاحصات الفيروسات "(Virus scanners) ملف بصمات الفيروسات لمقارنته بالملفات الموجودة على القرص لاكتشاف وجود الفيروس. وهذا الملف هو عبارة عن قاعدة بيانات تحتوي على بصمة كل الفيروسات المعروفة وخصائصها. هذه الخصائص تتضمن عينات من الأوامر المستخدمة في برنامج الفيروس، وأنواع الملفات التي يتخصص الفيروس في إصابتها، وغير ذلك من المعلومات التي تفيد في اكتشاف الفيروس.

كما أن فاحصات الفيروسات تستطيع كذلك تنظيف الجهاز من الفيروس المكتشف. ولكن المشكلة الأساسية في هذا النوع أنه لا يكتشف إلا الفيروسات المسجلة لديه، ومن ثم يجب تحديثه باستمرار بإضافة بصمات الأنواع الجديدة المكتشفة من الفيروسات. وتزداد الأمور صعوبة مع الفيروسات ذات الأوجه المتعددة التي تغير من بصمتها باستمرار، كما أن الملفات المضغوطة أو المشفرة يمكن أن تشكل مشكلة لهذا النوع من الفاحصات.

وبعض هذه الفاحصات يتم تركيبه ليكون مقيماً في الذاكرة باستمرار حتى يكون في مقدوره فحص أي برنامج يحاول التشغيل، والفاحصات المقيمة بالذاكرة لا تحتل جزءًا كبيرًا من الذاكرة، ويراعي صانعوها ألا تؤثر على الأداء.

٦-٣-٥ فاحص الفيروسات (Heuristic):

هناك نوع من فاحصات الفيروسات وهو (Heuristic scanner) الذي يجري تحليلاً إحصائيًا يساعده في تحديد احتمالات وجود فيروس داخل البرنامج المفحوص، فهذا النوع لا يقارن بصمات الفيروسات ولكنه يعطي درجة (نسبة مئوية) لاحتمال أن يكون هناك فيروس، فإذا تجاوزت هذه الدرجة حدًا معينًا أعلن عن وجود الفيروس. ويمتاز هذا النوع بعدم الحاجة إلى تحديثه، وتحتوي معظم برامج مكافحة الفيروسات الحالية على هذه الإمكانية، ولكن يعيبها أنها كثير ما تصدر إنذارات عما تعتقد أنه فيروس بينما لا يكون هناك فيروس في الحقيقة.

٦-٣-٦ فاحص فيروسات التطبيقات (Application-level virus scanner):

هذا النوع الجديد من فاحصات الفيروسات (Application-level virus scanner) مسئول عن تأمين خدمة معينة (تطبيق معين) في الشبكة وليس عن تأمين جهاز معين. فالبريد الإلكتروني مثلاً، وهو يشكل بيئة خصبة لنمو وانتقال الفيروسات، يمكن مراقبته بأحد هذه الأنواع ومن أمثلته برنامج (Inter-Scan Virus Wall) من شركة (Trend Micro) الذي يقوم بفحص أي ملحقات لرسائل البريد الإلكتروني.

٦-٤ مواصفات برامج مكافحة الفيروسات:

يجب أن تتمتع برامج مكافحة الفيروسات بالمواصفات التالية:

- القدرة على العمل في خلفية نظام التشغيل، وأن تقوم بشكل آلي بفحص البريد

الإلكتروني وأي ملفات يقوم المستفيد باستحضارها من شبكة الإنترنت أو أي شبكة يتصل بها.

- القدرة على أن تقوم آليًا بفحص أي قرص مرن (Floppy) أو قرص مضغوط (CD) وغيرها قبل نسخها أو تشغيلها.
- القدرة على الجدولة الآلية لعمليات الفحص الشامل للقرص الصلب.
- القدرة على العمل بشكل آلي عند تشغيل النظام (System startup)، وعند إنهاء النظام (System shutdown)
- أن تصدر تنبيهًا في حالة عدم تحديثها.
- أن تقوم آليًا بعملية تحديث نفسها من خلال الاتصال بشبكة الإنترنت باستحضار ملفات بصمات الفيروسات الجديدة.
- القدرة على إنشاء قرص تشغيل (Boot disk) نظيف مقاوم للفيروسات، ليمكن تشغيل النظام من خلاله، ثم تشغيل نظام مكافحة الفيروسات لفحص الجهاز عند حدوث أي مشكلة.

٦ـ٥ مستقبل الفيروسات:

للأسف، يبدو مستقبل الفيروسات مشرقًا! فقد أدلى خبراء أمن المعلومات بشهادتهم أمام اللجنة الفرعية للعلوم التي شكلها الكونجرس الأمريكي في منتصف عام ٢٠٠٠م فحذروا الكونجرس من أنه لا يمكن عمل شيء حاسم لمنع انتشار فيروسات الحاسبات في المستقبل القريب، وأنهم يتوقعون أن تكون فيروسات المستقبل أخطر من فيروس " مليسا " (Melissa virus) وفيروس " جرثومة الحب " (Love bug) [Bentley ٢٠٠٠] وألمحت هذه اللجنة إلى أن الحكومة الأمريكية نفسها (وكالة ناسا للفضاء، ووكالة المخابرات المركزية، ووزارة الطاقة) قد تعرضت أجهزتها لهجمات الفيروسات أكثر من مرة. وهناك اتجاه كبير لدعم أبحاث مكافحة الفيروسات خاصة تلك التي تنتشر عبر

شبكة الإنترنت، توقعًا لهجمات شرسة بالفيروسات ودود الكمبيوتر. وهذا النوع الجديد المتوقع لا يحتاج إلى تدخل البشر لانتشاره، وهنا تكمن خطورته، فالمستفيد لن يستطيع مع هذا النوع حماية نفسه بمجرد عدم فتح الملفات المشبوهة التي ترافق البريد الإلكتروني، أو تجنب استخدام بعض أنواع الماكرو أو (Scripts) وسوف تتمتع دودة الكمبيوتر في المستقبل بالخصائص التالية:

- القابلية للعمل في بيئات مختلفة، وأنواع متعددة من الحاسبات.
- القابلية للتخفي فيصعب اكتشافها.
- القابلية للانتشار دون تدخل المستفيد.
- القدرة على تعلم أساليب جديدة وتلقينها لأنواع الدود الأخرى.
- الحصانة ضد التتبع أو التعديل أو التدمير.
- القدرة على التلون وتغيير البصمة باستمرار.

في هذا الفصل استعرضنا الفيروسات بأنواعها وبينا مدى خطورتها وكيفية مواجهتها. وقبل أن نختم هذا الفصل نود أن نؤكد أن مسئولية الحماية من الفيروسات مسئولية مشتركة يجب أن يتعاون فيها العديد من الأطراف. لذلك نود توجيه الدعوة لمقدمي خدمة الإنترنت بتوفير برمجيات فحص ومكافحة الفيروسات على أجهزة الخدمة الخاصة بهم حماية للمشتركين.



الفصل السابع
تقنيات الحماية

بعد أن استعرضنا في الفصل الخامس أساليب انتهاك شبكات المعلومات، واستعرضنا في الفصل السادس موضوع الفيروسات وتهديدها لشبكات المعلومات، فإن هذا الفصل خصصناه لدراسة التقنيات الحديثة المستخدمة في حماية المعلومات، فنبدأه باستعراض تقنيات التشفير بادئين بمفهوم التشفير (التعمية) وأهميته ثم بالتمييز بين التشفير المتماثل والتشفير غير المتماثل، ثم متطلبات البنية الأساسية للمفتاح العلني (Public key infrastructure).

في القسم الثاني من هذا الفصل نتحدث عن " التوقيعات الرقمية "(Digital signatures)، بينما نخصص القسم الثالث لشهادات التعريف الرقمية (Digital certificates)، وسلطات منح هذه الشهادات (Certification authorities)، وبعض الاستخدامات العملية للشهادات الرقمية.

ونستعرض في القسم الرابع الأغلفة الرقمية، ثم نستعرض في القسم الخامس الأنواع الأربعة من الأجهزة والتقنيات الحديثة التي تستخدم في مراقبة الشبكات: تحديد الشخصية والتحقق منها، والتحكم في السماح بالاستخدام، وفاحصات النظم، وكشف الاقتحام والمراقبة.

ثم نختتم بالحديث عن التقنية الشائعة الاستخدام " الخصوصية الفائقة " (Pretty Good Privacy) لحماية البريد الإلكتروني وأسلوب بنية الطبقات الثلاث (Three- tier structure).

٧-١ مفهوم التشفير (التعمية) وأهميته:

٧-١-١ مفهوم التشفير (Encryption):

بفرض أن لدينا رسالة نود إيصالها إلى شخص ما ولكننا نخشى من وقوع رسالتنا هذه في يد طرف ثالث لا ينبغي أن يطلع عليها. في هذه الحالة نقوم " بتعمية " الرسالة (لفظ التعمية هو اللفظ العربي القديم المستخدم للتعبير عن الرسائل المشفرة) بحيث لو

تم اعتراض الرسالة المنقولة فلا ينكشف مضمونها. هذا باختصار هو (التشفير Encryption) وهو وسيلة الحفاظ على أمن المعلومات في بيئة غير آمنة.

ربما كان التشفير هو أهم حجر في بناء أمن المعلومات ولكنه ليس الحجر الوحيد على أية حال. ويقول " بوير " أن أكثر وسائل أمن المعلومات فعالية هي " التشفير " ويعرفه على النحو التالي: (تشفير المعلومات هو تغيير مظهرها بحيث يختفي معناها الحقيقي) [Bower ١٩٩٦]. فعن طريق تحوير صورة البيانات، بحيث تكون غير مفهومة لمن يتلصص عليها، يستطيع إخصائيو أمن المعلومات منع الأشخاص غير المرخص لهم من الاطلاع على هذه البيانات، وبذلك يحقق التشفير سرية البيانات. كما أن التشفير يمكن استخدامه بهدف تحقيق سلامة البيانات لأن البيانات التي لا يمكن قراءتها لا يمكن بالتالي تعديلها أو تزييفها. ويستخدم التشفير الآن كأساس لبعض البروتوكولات (مجموعة متتالية متفقّ عليها من الأفعال لتنفيذ مهمة معينة) التي تضمن إتاحة الموارد لمن يحتاج إليها.

يتضح من ذلك أن التشفير يقع في موقع القلب من وسائل ضمان أهداف أمن المعلومات الثلاثة وهي: (خصوصية البيانات Data Confidentiality) و(سلامة البيانات Data Integrity) و (إتاحة البيانات Data Availability).

وبرغم أن التشفير يعتبر أداة هامة من أدوات أمن المعلومات إلا أننا يجب ألا نبالغ في هذه الأهمية، فالتشفير لا يحل جميع مشاكل أمن المعلومات. علاوة على ذلك فإذا لم يستخدم التشفير بالشكل المناسب، فقد لا يكون فعالاً في تأمين البيانات، أو قد يؤدي إلى سوء أداء النظام ككل. فالتشفير الضعيف يمكن أن يكون بالفعل أسوأ من عدم التشفير لأنه قد يعطي إحساسًا زائفًا بالأمن، لذلك فمن الأهمية بمكان أن نعرف المواقف التي يكون التشفير فيها مفيدًا وأن نستخدمه بكفاءة [داود ٢٠٠٠أ].

٧ـ١ـ٢ الأخطار التي يمكن التغلب عليها بواسطة التشفير:

يستخدم التشفير للتغلب على الأخطار التالية:

(١) الاطلاع على المعلومات المحظورة.

(٢) محاولات تعديل البيانات المنقولة بالشبكة.

(٣) إعادة توجيه البيانات إلى وجهة أخرى.

(٤) تأخير إيصال بعض الرسائل.

(٥) تغيير محتويات الرسائل المتبادلة.

(٦) إقحام رسائل زائفة ضمن الرسائل المنقولة عبر الخط.

(٧) تغيير كلمات السر الخاصة بالمستفيدين.

(٨) انتحال شخصية المستخدم الحقيقي.

(٩) تعديل البيانات المخزنة على الحاسبات نفسها.

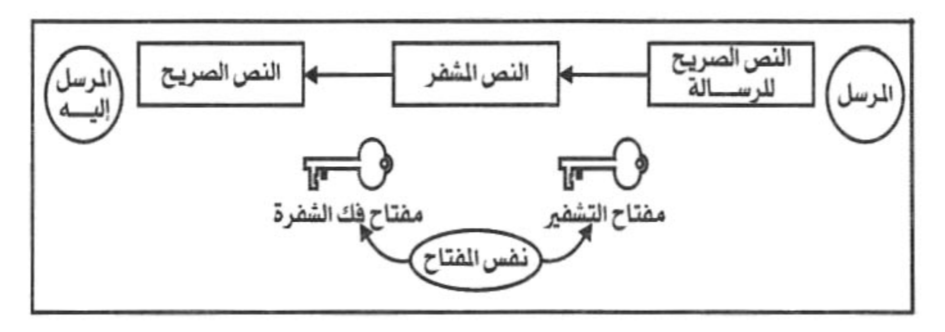
٧ـ١ـ٣ تقنيات التشفير:

التشفير علم قديم وعلم حديث في الوقت نفسه، علم ولد منذ زمن بعيد، وتطور بشكل مذهل بعد انتشار استخدام الحاسب الآلي بسرعته الهائلة وقدراته العظيمة على المعالجة. ويمكن الاستفادة من هذا العلم لتحقيق الخصوصية وسرية المعلومات عن طريق تشفير الرسائل قبل إرسالها، ثم فك شفرتها عند استلام الرسالة. وفي غياب مفتاح الشفرة تكون الرسالة لا معنى لها، فلو استطاع شخص دخيل أن يحصل على الرسالة المشفرة قبل أن تصل إلى المرسل إليه دون أن يكون لديه مفتاح الشفرة فإن الخصوصية والسرية لا تنتهكا. وسنقصر حديثنا في هذا الفصل على دور التشفير في تحقيق الأمن لشبكات المعلومات.

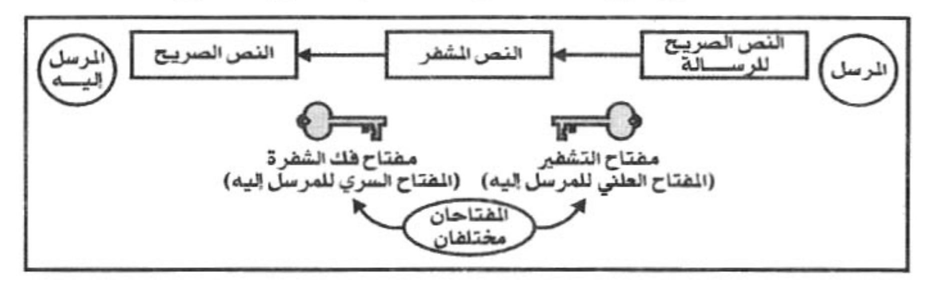
٧-١-٤ التشفير المتماثل وغير المتماثل:
(Symmetric & Asymmetric cryptography)

هناك أسلوبان لتشفير المعلومات المارة في شبكات المعلومات وهما: " التشفير المتماثل " (Symmetric cryptography) أو ما يطلق عليه أسلوب " المفتاح السري " حيث يستخدم مفتاح واحد لكل من تشفير الرسالة وفك شفرتها، الشكل (٧-١). الأسلوب الثاني هو أسلوب " التشفير غير المتماثل "(Asymmetric cryptography) أو ما يطلق عليه أسلوب " المفتاح العلني "(Public key)، حيث يستخدم مفتاح للتشفير ومفتاح آخر لفك الشفرة، الشكل (٧-٢).

شكل (٧-١)
التشفير المتماثل باستخدام المفتاح السري



شكل (٧-٢)
التشفير غير المتماثل باستخدام المفتاح العلني



والأسلوب المتماثل (المفتاح السري) غير كاف للتأكد من الشخصية، فحصول شخص ما على المفتاح ليس دليلاً كافيًا على أنه هو الشخص المقصود بالرسالة، وحصول شخص غير معني على المفتاح لا يتيح له فقط فك شفرة الرسالة، ولكن يسمح له كذلك باختلاق رسالة جديدة باستخدام هذا المفتاح، مما يحدث ثقبًا واسعًا في جدار الأمن. وهذا هو السبب الذي من أجله يواصل الجميع تغيير مفتاح الشفرة وكلمات السر من آن لآخر، لأن وقوع المفتاح في يد غريبة أو كسره بواسطة البرامج المتاحة حاليًا، لم يعد أمرًا بعيد الاحتمال، خاصة مع التقدم السريع والمستمر في قدرات الحاسب الآلي والتي دفعت إلى تطوير أساليب تشفير أقوى، ومفاتيح تشفير تكاد تستعصي على الكسر.

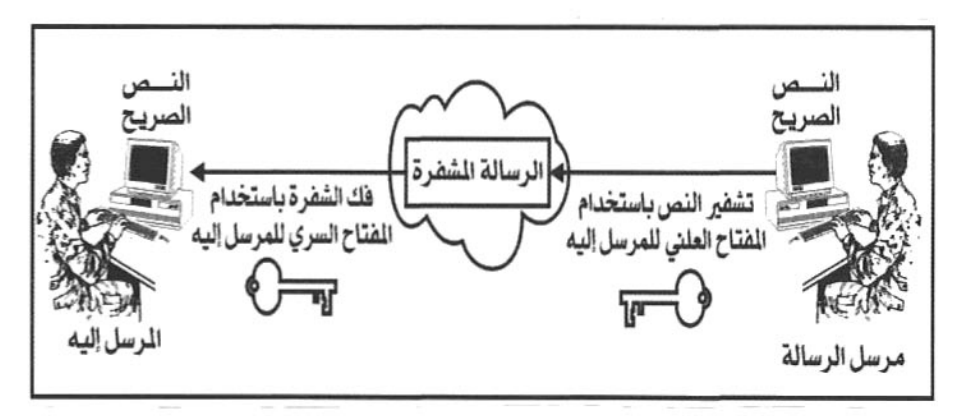
ومن المهم أن نعلم أنه كلما زاد طول المفتاح، أي عدد الخانات (Bits) التي يتكون منها، ازداد المفتاح مناعة وازدادت صعوبة كسر الشفرة باستخدام الطرق العشوائية [داود ٢٠٠٠ب]، فنظرية الاحتمالات تقول أن عدد المفاتيح المحتملة هو($٢^{ن}$)، حيث " ن " هو عدد الخانات (Bits)التي يتكون منها مفتاح الشفرة، أي أن المفاتيح المحتملة لشفرة طولها ٨ خانات هو ٢٥٦ احتمالاً ($٢^{٨}$). وأكثر أنواع هذا الأسلوب انتشارًا هو نظام التشفير الرقمي (DES) أو (Digital Encryption Standard) الذي يستخدم ٥٦ خانة، ولنبين أهمية طول المفتاح فإن مفتاحًا طوله ٥٦ خانة يبلغ عدد احتمالاته $٧,٢ \times ١٠^{١٦}$ احتمالاً، ولكي يتم كسر شفرته عن طريق التجربة العشوائية لا يمكن أن يتم ذلك باستخدام الحاسبات العادية، ولكن يلزم استخدام تقنيات خاصة مكلفة جدًا للمعالجة المتوازية (Parallel processing). ويتفق معظم الخبراء على أن الشفرة التي طولها ١٢٨ خانة (Bits)، والتي تحتاج إلى تجربة احتمالات عددها $٣,٤ \times ١٠^{٣٨}$ احتمالاً، هي شفرة آمنة تمامًا (على الأقل في المستقبل المرئي).

وبسبب طول مفاتيح الشفرة يلزم تبادلها عن طريق وسط إلكتروني، كأن نخزنها على قرص ونعطيها للطرف الآخر، أو نرسلها له بالبريد الإلكتروني، ولكن كيف نضمن عدم تسرب المفتاح في هذه الحالة؟ جاءت إجابة هذا السؤال في عام ١٩٧٥ على يد

" وتفيلد ديفي " و" مارتن هلمان " عندما اقترحا استخدام " التشفير غير المتماثل " حيث يكون لكل شخص زوجان من المفاتيح: أحدهما سري (Private) والآخر علني (Public)، وهما مشتقان من أصل واحد، ولكن المفتاح السري لا يمكن استنتاجه من المفتاح العلني، إذ يختلف أسلوب اشتقاق المفتاح السري عن أسلوب اشتقاق المفتاح العلني. وأشهر النظم التي تعتمد على المفتاح العلني هو نظام (RSA)، الذي جاءت تسميته تبعًا لمخترعيه الثلاثة (رون رايفست وآدي شامير وليونارد أدلمان). ويمكن استخدام هذا النظام بأن تعطي مفتاحك العلني للشخص الذي تريد مراسلته، ويستطيع هذا الشخص أن يستخدم مفتاحك العلني في تشفير الرسالة التي يود إرسالها إليك. وهذه الرسالة لا يمكن فك شفرتها إلا باستخدام مفتاحك السري، يعني لا يستطيع قراءتها سواك، ويبدو ذلك في الشكل (٧-٣). وهذه كانت أول خطوة للوصول إلى التوقيعات الرقمية (Digital signatures)

شكل (٧-٣)

إرسال رسالة مشفرة باستخدام المفتاح العلني

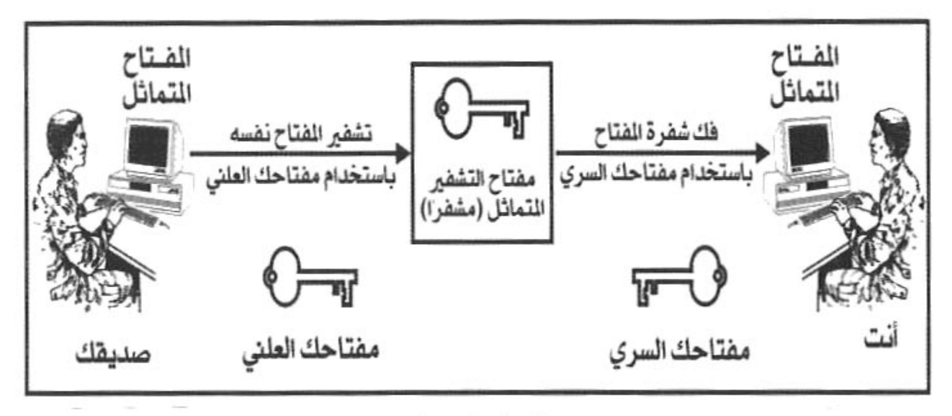


نظرًا لأن الأسلوب غير المتماثل (المفتاح العلني) قد يؤثر على أداء الحاسب، لأنه يستغرق وقتًا أطول في التشفير وفي فك الشفرة، فكثيرًا ما يتم استخدام الأسلوب المتماثل (المفتاح السري) في تشفير الرسالة لأنه أسرع بكثير، بينما يستخدم أسلوب

المفتاح العلني في تشفير المفتاح السري المستخدم في تشفير الرسالة، ويتم التعامل على النحو المبين في شكل (٧-٤) وشكل (٧-٥).

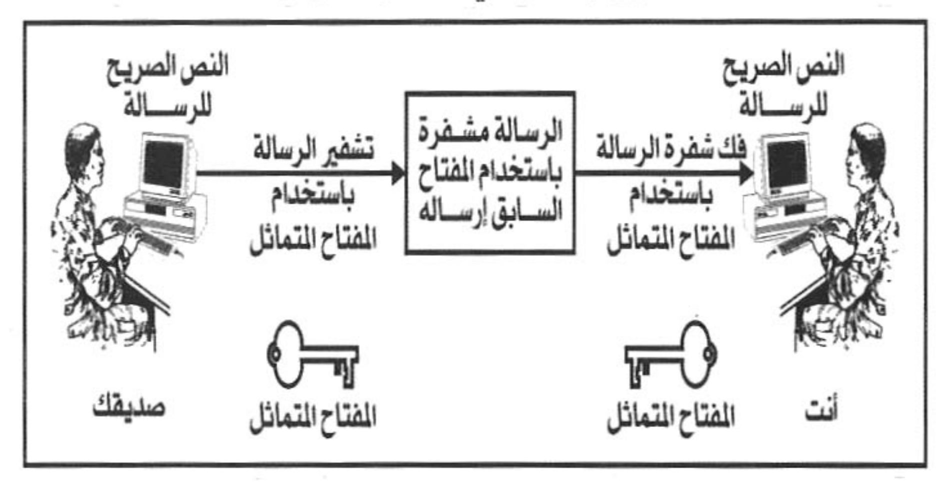
شكل (٧-٤)

الخطوة الأولى : تشفير مفتاح الشفرة المتماثل باستخدام أسلوب المفتاح العلني (غير المتماثل)



شكل (٧-٥)

الخطوة الثانية : تشفير الرسالة باستخدام أسلوب المفتاح المتماثل الذي سبق إرساله في الخطوة الأولى



عند بدء الاتصال يقوم صديقك باستخدام مفتاحك العلني لتشفير مفتاح تشفير الرسالة، ثم يرسل المفتاح المشفر إليك، فتقوم أنت بفك شفرته (باستخدام مفتاحك السري)، فتحصل بذلك على مفتاح تشفير الرسالة المتماثل. ثم يرسل لك صديقك الرسالة مشفرة بهذا المفتاح المتماثل الذي حصلت عليه في الخطوة السابقة فتقوم بفك شفرتها باستخدامه.

للتأكد من أنك أنت بالفعل الذي حصلت على المفتاح المتماثل (السري) وليس أحد آخر يتم اتباع خطوة تأكيدية زائدة عند إرسال مفتاح التشفير فيتم اتباع التالي:

١- يقوم صديقك بتوليد مفتاح مماثل (باستخدام برنامج على جهازه)، ثم يقوم باستخدام مفتاحك العلني في تشفير هذا المفتاح، ثم يقوم بإرساله إليك.

٢- تقوم أنت (باستخدام مفتاحك السري) بفك التشفير والحصول على المفتاح، ثم تقوم (باستخدام مفتاح صديقك العلني) بتشفير نفس المفتاح الذي وصل إليك ثم تعيد إرساله إلى صديقك، الذي يقوم بفك شفرته (باستخدام مفتاحه السري) ويطابق المفتاحين.

الآن يستطيع كل منكما استخدام هذا المفتاح في التراسل بينكما باستخدام أسلوب التشفير الأكثر سرعة وهو التشفير المتماثل.

وإحدى الخصائص المهمة لنظام (RSA) للتشفير باستخدام المفتاح العلني، هي أن كلا المفتاحين يمكنه فك شفرة أي نص تم تشفيره بالمفتاح الآخر. أي أن المفتاح السري يمكنه فك شفرة الرسالة التي تم تشفيرها بواسطة المفتاح العلني، والعكس بالعكس. ولكن هنا تبرز مشكلة، فإنك إذا استخدمت مفتاحك السري لتشفير رسالة، فإن أي شخص يمكنه قراءتها باستخدام مفتاحك العلني، ولكن هذه النقطة تعتبر ميزة مهمة من ناحية أخرى، فإذا قمت بتشفير رسالة ما باستخدام مفتاحك السري، فإن متلقي الرسالة سوف يكون متأكدًا من أنك أنت، ولا أحد سواك، الذي قام بإرسال هذه الرسالة. ولكن كيف يتحقق من أن حائز المفتاح السري هو أنت نفسك؟ وأنك أنت من

بدأ الاتصال وليس طرفًا دخيلاً؟ هذه النقطة بالذات هي التي تظهر فيها على مسرح الأحداث " سلطات منح الشهادات الرقمية " (Certification authorities) وهي ما سنتطرق إليها بالتفصيل في هذا الفصل.

٧-١-٥ أسلوب التشفير المودع (EEs):

أسلوب (التشفير المودع Escrowed Encryption System) أو (EES) هو نظام تشفير يعتمد على المفتاح السري، وقد تم تطويره بواسطة الحكومة الأمريكية وقد شارك في تطويره كل من " سكيب جاك " و" كليبر " و" كابستون "، وهذان الأخيران قاما بإعداد رقاقة تحتوي على النظام سميت (رقاقة كابستون Capstone Chip) ورقاقة أخرى سميت (رقاقة كليبر Clipper Chip)، وكل من الرقاقتين تستخدمان خوارزمية (سكيب جاك Skipjack Algorithm)، ومن شأن هذه الرقاقات أن تسهل استخدام هذا الأسلوب (EES) مع نظام كنظام الهاتف مثلاً لتشفير المكالمات الهاتفية. وتعتبر تفاصيل خوارزمية (EES) من الأسرار الاستراتيجية للولايات المتحدة الأمريكية [Pfleeger ١٩٩٧].

في عام ١٩٩٢م أعلنت شركة " إيه تي أند تي " (AT&T) عن إنتاج جهاز هاتف يسمح بتشفير الاتصالات الصوتية (وخاصة الهاتفية منها) [Denning ١٩٩٣] ويتم ذلك بتحويل المكالمة أولاً إلى إشارة رقمية (Digital) ثم تشفيرها ثم إعادة تحويل النص المشفر إلى إشارة تناظرية (Analog) لنقلها عبر شبكة الهاتف الصوتية ، ثم عكس هذا الإجراء لدى الطرف المستقبل لفك الشفرة. وكان في مقدور هذه الأجهزة توليد مفتاح شفرة جديد في كل محادثة وتشفير المفتاح نفسه ثم إرساله إلى الجهاز المستقبل قبل إجراء المحادثة المشفرة.

وقد سبب هذا المنتج عند ظهوره مشاكل كثيرة للجهات الأمنية وللشرطة مما منعها من متابعة العصابات الإجرامية، برغم حصولها على إذن من القضاء بالمتابعة

والتنصت. ولذلك تم تعديل هذا المنتج فيما بعد، بحيث تستطيع الأجهزة الأمنية أن تكسر هذا النوع من التشفير دون الحاجة إلى إضعافه فيتمكن الآخرون من كسره. وكان الدافع الرئيسي وراء إنتاج نظام (EES) هو ما ثار حول نظام (DES) من شكوك مع تطور العتاد وازدياد سرعة المعالجة، وما صاحب ذلك من انتشار واسع لأسلوب المفتاح العلني في التشفير (خاصة نظام RSA) مما جعل الجهات الأمنية تخشى من استخدام العصابات الدولية لنظام (RSA) مع مفاتيح صعبة الاختراق، ولذلك تم التوصل إلى نظام (EES) بحثًا عن أمرين: الأمر الأول هو الحصول على شفرة أقوى، والثاني هو تمكين الشرطة من كسر شفرة الرسائل المشفرة .

يتم عند استخدام هذا النوع من التشفير إيداع مفاتيح الشفرة لدى أي وكالة موثوق بها، ولحماية أمن التشفير يمكن تقسيم المفتاح إلى أجزاء بحيث يتم إيداع كل جزء لدى وكالة معينة. وعند صدور حكم من المحكمة بمراقبة محادثة معينة تأتي هذه الوكالات بأجزاء المفتاح التي لديها وتسلمها للشرطة التي تتولى إدخالها إلى جهاز فك التشفير حتى يمكن التنصت على المحادثة.

ويمكن الرجوع إلى كتاب " الحاسب وأمن المعلومات " من إصدارات معهد الإدارة العامة [داود ٢٠٠٠أ] للمزيد من المعلومات حول أساليب التشفير.

٧-١-٦ البنية الأساسية للمفتاح العلني(PKI):

الاتجاه الآن هو نحو استخدام " سلطات منح شهادات تعريف المفتاح العلني " (Public- key certification authorities) لإثبات شخصية المتعاملين على شبكة الإنترنت. وبدون إنشاء البنية الأساسية للمفتاح العلني (PKI) أو (Public Key Infrastructure) لا يمكن استخدام هذا الأسلوب بنجاح.

ومن بين مكونات هذه البنية الأساسية نجد: " سلطات منح الشهادات الرقمية " (Certification authorities)، و" التوقيعات الرقمية " (Digital signatures)، و"

الرسائل المركزة " (Message digests) المستنتجة من الرسالة الأصلية بواسطة خوارزمية القيمة الاختبارية (Hash)، بالإضافة إلى أسلوب " التشفير باستخدام المفتاح العلني " (Public key cryptography).

والهدف من هذه البنية الأساسية هو تسهيل تأكيد شخصية أي شخص على شبكة الإنترنت، فلابد أن تتحقق " سلطة منح الشهادات الرقمية " (Certification authority) من شخصية من يتقدم بطلب الحصول على شهادة التعريف، ومن ثم تصدر له هذه الشهادة، كما تتولى متابعة حالة هذه الشهادة وما قد يطرأ عليها من تغيير، وما يطلب بشأنها من تأكيد، فمن حق أي شخص أن يطلب التأكد من الشهادة التي تعرِّف أي شخص آخر. وسنتحدث بالتفصيل في هذا الفصل عن كل من " التوقيعات الرقمية " (Digital signatures) و" سلطات منح الشهادات الرقمية "(Certification authorities).

من المفروض عند اعتماد دولة ما للبنية الأساسية للمفتاح العلني (كما تتجه المملكة العربية السعودية) أن يتم استخدام أسلوب المفتاح العلني في تعريف جميع الأطراف المتعاملة، ولكن هذا لا يحدث للأسف دائمًا، فبعض الجهات تهتم بتأكيد الشخصية لطرف واحد فقط، وهو جمهور المتعاملين مع الجهة.

هناك مجالات أساسية ثلاثة لاستخدام المفتاح العلني، وهي تشكل جزءًا من البنية الأساسية الخاصة به (PKI)، وذلك نظرًا لكفاءته ومناعته ضد الكسر ونظرًا لوجود أجهزة (Hardware) تعتمد عليه بحيث يتم التشفير وفك الشفرة بشكل آلي تمامًا. هذه المجالات الثلاثة هي:

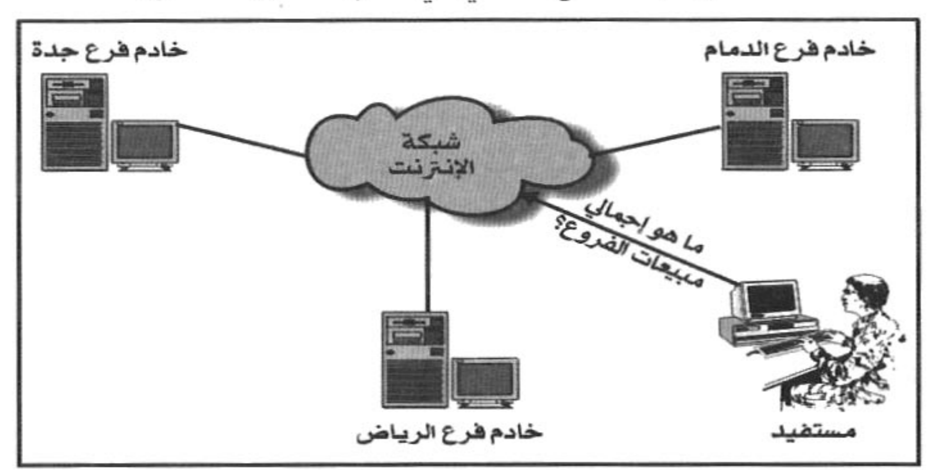
(١) **تعريف الشخصية:** وهو أهمها حيث تتعرف خوادم الشبكة (Web servers) على المستفيدين، وكذلك يتأكد المستفيد من هوية خادم الموقع الذي يتعامل معه.

(٢) **تأمين الاتصال بين النظم:** وهو أكثرها انتشارًا الآن، إذ تستخدم كثير من المؤسسات بروتوكول (SSL) أو (Secure Sockets Layer)الذي طورته شركة " نت سكيب "(Netscape communications)، حيث يتم استخدام المفتاح العلني في

تـأمين عمليـة تبادل المفـاتيح السـرية (وليـس في تشفيـر البيانـات نفسهـا). في هذه الحـالة، وعـند الـدخول إلـى موقع مـؤمن، فـإن عنـوان الموقع (URL) سيكـون مثلا (https://www.xyz.com) بــدلاً مـن (http://www.xyz.com) وهــو العنـــوان المستخدم مع المـواقع غير المؤمنة، ويـلاحظ القارئ وجـود حرف (s) في نهـاية اسم البروتوكول (https)

(٣) **سلامة وتكامل التطبيقات:** هـذا الاستخـدام الحديث للمفتـاح العلني يـضمن سلامة وتكامل الأجـزاء البعيدة من النظم الموزعة، ففي هذا النوع من النظم (الموزعة) قد تجد تطبيقًا تتشعب أجزاؤه على أجهزة مختلفة في الشبكة، فكيف يتأكد كل جزء من أجزاء التطبيق من صحة البيانات المرسـلة إليه من الجزء الآخر؟ هنا، ومن خلال التشفير باستخـدام المفتاح العلنـي، يمكن تنفيذ هـذا التأكيـد. ويبين الشكل (٧-٦) كيفية استخدام بنـية المفتـاح العلني (PKI) في تأمين الـتطبيقـات الموزعـة. في هذا المثـال يوجه المستفيد استفسارًا يـطلب معرفة إجمالـي مبيعات الفروع، فـيطلب التطبيق، من خلال الإنتـرنت، معلـومات من كل فـرع من فروع المؤسسـة. في هذه الحالة تـطلب الفروع تأكيـدًا لشخصيـة الخادم الذي وجه الاستفسار، ويتم ذلك عن طريق المفتاح العلني.

شكل (٧-٦)
استخدام بنية المفتاح العلني في تأمين التطبيقات الموزعة



٧-٢ التوقيعات الرقمية (Digital signatures):

رأينا في القسم السابق كيف أن استخدام " المفتاح العلني " قد حل مشكلة ضمان عدم قراءة الرسائل إلا بواسطة المرسل إليه الذي لديه المفتاح السري اللازم لفك شفرة الرسالة، كما حل مشكلة إرسال مفتاح الشفرة عن طريق المفتاح العلني، الذي يستخدم في تشفير الرسالة، والذي لا يمكن منه استنتاج المفتاح السري. ولكن بقيت مشكلة واحدة وهي تأكد مستلم الرسالة من شخصية مرسلها، فالمفتاح العلني متاح للجميع، فكيف إذًا يمكن التأكد من أن مرسلها هو من وضع اسمه في حقل المرسل؟ وكيف يمكن التأكد من أن هذه الرسالة لم يطرأ عليها تعديل خلال رحلتها عبر الشبكة أو الشبكات التي مرت بها؟ الحل يكمن في " التوقيع الرقمي " (Digital signature).

٧-٢-١ مفهوم التوقيع الرقمي:

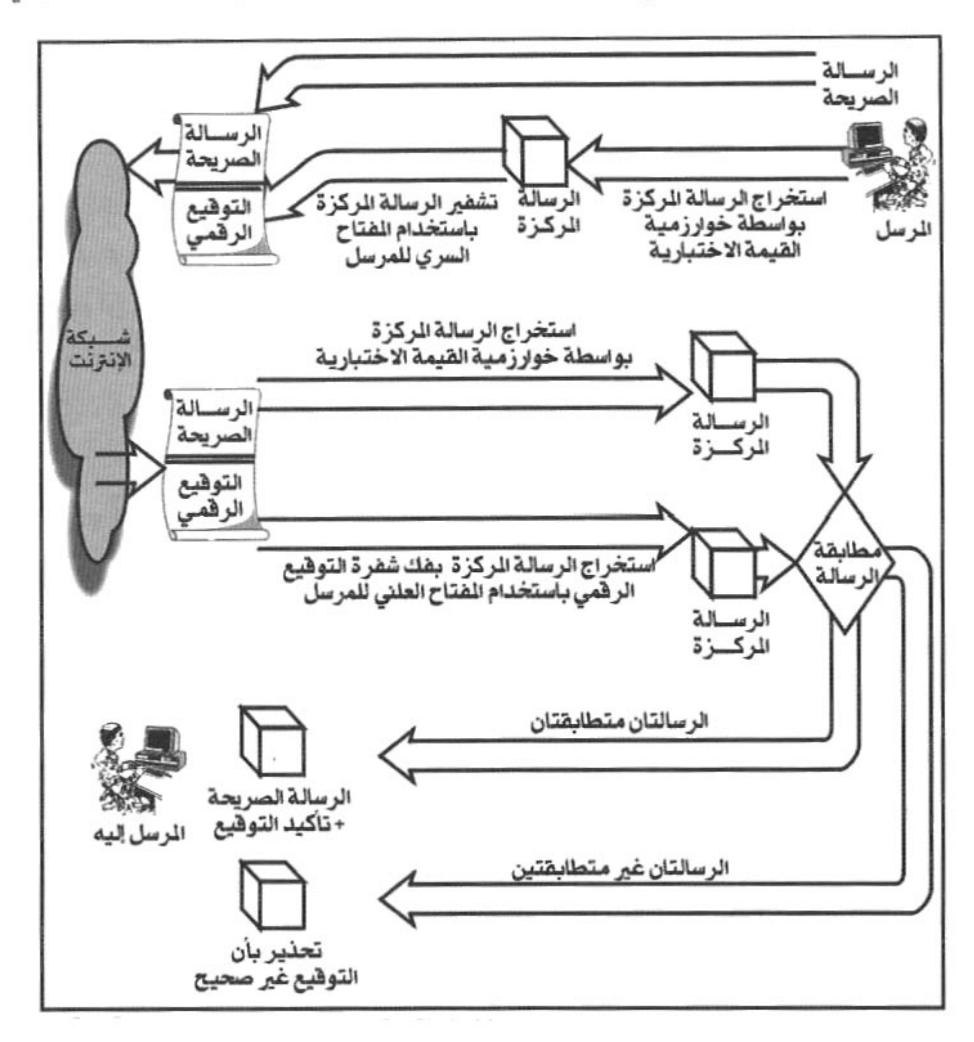
لكي نفهم ما يمكن أن يفعله التوقيع الرقمي دعنا نتصور الافتراض التالي: إذا استخدم مرسل الرسالة مفتاحه السري لتشفير هذه الرسالة، فإن المستقبل عندما يفك

شفرة الرسالة باستخدام المفتاح العلني للمرسل، سوف يكون متأكداً من أن هذه الرسالة مرسلة بالفعل من جانب المرسل، ذلك لأن المرسل وحده دون غيره هو الذي يعرف مفتاحه السري الذي استخدم في تشفير الرسالة.

ولكننا نذكر أنه في نظام التشفير باستخدام المفتاح العلني، فإن ما يتم تشفيره بالمفتاح السري يمكن فك شفرته بالمفتاح العلني، والعكس بالعكس. يعني ذلك أن أي شخص يحصل على المفتاح العلني لمرسل الرسالة يستطيع فك شفرتها التي استخدم فيها المفتاح السري. وهذا قد يؤثر على سرية الرسالة التي قام مرسلها بتشفيرها باستخدام مفتاحه السري، وللتغلب على هذه المشكلة فإن التوقيع الرقمي لا يتم بتشفير الرسالة المرسلة كلها، ولكن يتم تشفير " القيمة الاختبارية " (Hash) للرسالة (تحدثنا في الفصل الخامس عن القيمة الاختبارية وكيفية الحصول عليها من نص الرسالة). وهذه القيمة الاختبارية هي مجموعة من الحروف أصغر كثيراً من الرسالة الأصلية، ١٦٠ خانة (Bit) مثلاً.

شكل (٧-٧)

استخدام " التوقيع الرقمي " لضمان سلامة الرسائل ونسبتها إلى مرسلها الحقيقي



يبين شكل (٧-٧) مخرجات خوارزمية القيمة الاختبارية والتي تسمى أحيانًا " الرسالة المركزة " (Message digest) حيث يتم تشفير هذه الرسالة المركزة باستخدام المفتاح السري للمرسل لتنتج " التوقيع الرقمي "، ثم يتم إرسالها مع الرسالة الصريحة

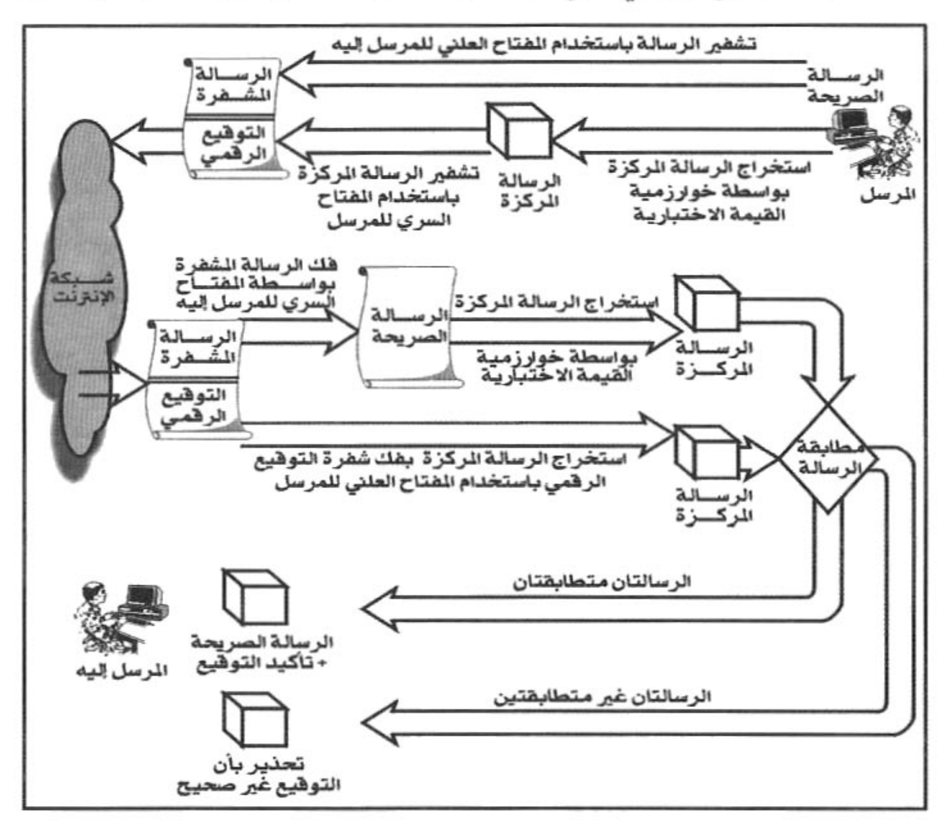
عبر الشبكة. يقوم المستقبل بفك شفرة " التوقيع الرقمي " باستخدام المفتاح العلني للمرسل لتظهر " الرسالة المركزة " في صورتها غير المشفرة. كما يقوم بتنفيذ خوارزمية القيمة الاختبارية على الرسالة الأصلية لإنتاج " الرسالة المركزة " عن طريق آخر. وهنا إذا تطابقت الرسالة المركزة المخرجة في كل من الحالتين فإن ذلك يكون كافيًا لإثبات أن هذه الرسالة مصدرها هو المرسل فعلاً (تم التشفير بواسطة مفتاحه الخاص) وأنها لم يحدث عليها تعديل (النص الوارد أخرج نفس الرسالة المركزة). أما إذا وجد عدم تطابق بين الرسالتين المركزتين فإنه يعني ضرورة رفض هذه الرسالة. ويتضح أن المرسل لا يستطيع إنكار إرساله هذه الرسالة. أي أن " الرسالة المركزة " ضمنت سلامة الرسالة الأصلية و" التوقيع الرقمي " ضمن سلامة " الرسالة المركزة " نفسها.

٧-٢-٢ تشفير الرسائل مع التوقيع الرقمي:

بقيت نقطة مهمة هنا وهي أن الرسالة المرسلة تم إرسالها مفتوحة وغير مشفرة. ولكن التغلب على ذلك ممكن، فيستطيع مرسل الرسالة، إن شاء، أن يقوم بتشفيرها باستخدام المفتاح العلني للمرسل إليه، والذي يستطيع فك شفرتها بواسطة مفتاحه السري عند الاستلام. ولكن هذه العملية لا علاقة لها بالتوقيع الرقمي. وبصفة عامة فإذا كانت محتويات الرسالة غير ذات أهمية وكانت الأهمية تكمن في توقيع المرسل وفي التأكد من عدم تزوير الرسالة، فليست هناك ضرورة لتشفير الرسالة. أما إذا كانت محتويات الرسالة على درجة من السرية فيمكن تشفيرها كذلك، كما يبدو من الشكل (٧-٨). ويلاحظ أن خوارزمية القيمة الاختبارية (Hash algorithm) يمكن أن تعمل على النص الصريح وعلى النص المشفر كذلك.

شكل (٧-٨)

استخدام " التوقيع الرقمي " مع الرسائل المشفرة لضمان درجة عالية من الأمن



يمكن تنفيذ هذه العملية بأكملها بشكل آلي من خلال بعض النظم الآلية مثل نظام " الخصوصية الفائقة " (Pretty Good Privacy) باستخدام الأمر التالي:

اسم المستفيد اسم ملف الرسالة -sea #pgp

علمًا بأنه على المستفيد في هذه الحالة إدخال " جملة السر " (Pass phrase) لتأكيد شخصيته لنظام (PGP)

وهذه النظم الآلية تتولى المهمة بالكامل: التشفير بكافة أنواعه، وفك الشفرة،

والإرسال والاستقبال، وتأكيد الشخصية، بحيث أن المستفيد لا يحتاج إلى أن يقوم بنفسه بأي عمل، أو أن تكون لديه خبرة مسبقة بأي من هذه الأمور.

٧-٢-٣ الاعتراف بالتوقيع الرقمي:

عند التوقيع على الرسائل الورقية فإننا نفترض ثلاثة افتراضات:

١- التوقيع هو التزام من الموقع بما ورد في الوثيقة.

٢- الوثيقة لن يتم تغييرها بعد توقيعها.

٣- التوقيع لا يمكن (نسخه) ونقله إلى وثيقة أخرى.

والقوانين والأعراف المحلية والدولية تضمن تحقق هذه الافتراضات الثلاثة. أما بالنسبة للرسائل الإلكترونية، فإن التوقيع الرقمي يضمن الافتراضات الثلاثة على النحو التالي:

(١) التوقيع الرقمي قد تم باستخدام المفتاح السري للمرسل، بمعنى أنه هو الذي وقع الوثيقة وأنه ملتزم بما ورد فيها.

(٢) التوقيع الرقمي مستنتج من النص الأصلي للرسالة (لأنه تم بتشفير الرسالة المركزة) مما يعني أن الوثيقة لم يتم تغييرها بعد استخراج التوقيع الرقمي.

(٣) التوقيع الرقمي مستنتج من نص الرسالة، أي أنه لا يمكن نسخه أو نقله إلى رسالة أخرى، وإلا فإنه بعد فك تشفيره لن ينتج نفس " الرسالة المركزة ".

وقد بدأت كثير من الدول حول العالم إصدار التشريعات اللازمة للاعتراف بالتوقيع الرقمي ليكون ملزماً للطرف الموقع، ويمكن الحصول على بيانات كاملة عن مواقف الدول المختلفة من هذا الموضوع من شبكة الإنترنت [Baker ٢٠٠٣]. وتشمل قائمة الدول التي أجازت التوقيع الرقمي الولايات المتحدة (معظم الولايات) وكندا والدانمارك وفرنسا وألمانيا وإيطاليا واليابان وماليزيا وبريطانيا. وقد أعدت مفوضية الأمم المتحدة لقانون التجارة العالمية (UNCITRAL) تشريعاً نموذجياً للتوقيع الرقمي يمكن اتباعه،

كما أعد الاتحاد الأوروبي دراسة كاملة حول النواحي القانونية المتعلقة بالتوقيعات الرقمية، كما وضعت منظمة التعاون والتنمية الاقتصادية (OECD) مجموعة من القواعد الإرشادية للدول التي بصدد إعداد تشريعات تتعلق بالخصوصية وتأكيد الشخصية، بما في ذلك التوقيعات الرقمية [Baker ٢٠٠٣].

٧-٣ "شهادات التعريف الرقمية" (Digital certificates):

مكننا التوقيع الرقمي من التأكد من أن مرسل الرسالة هو فعلاً كاتبها، ولكي نكون أكثر دقة، فإن التوقيع الرقمي يؤكد أن من في حوزته المفتاح السري لمرسل الرسالة هو الذي قام بإرسالها. ولكن من يضمن لنا أن المفتاح السري لم يتسرب؟ وأن شخصاً ما لم يحصل عليه بطريقة ما وقام بإرسال الرسالة مدعيًا صدورها من صاحب المفتاح السري؟ أي أننا في حاجة إلى الربط بين المفتاح السري وصاحبه، سواء كان شخصاً أو شركة، وإلا أصبحت الثقة في التوقيع الرقمي غير كاملة.

يكمن الحل في وجود طرف محايد " يشهد " بأن هذا المفتاح السري يخص المرسل، هذا الطرف هو " سلطة منح الشهادات الرقمية " (Certification Authority)، وهذه السلطة تمنح " شهادة تعريف رقمية " (Digital Certificate) وشهادة التعريف الرقمية هي ببساطة وثيقة تقول بأنه يمكن الثقة في مصدر هذه المعلومات، لأن صاحب المفتاح السري المستخدم في إعداد التوقيع الرقمي هو نفسه مرسل الرسالة.

٧-٣-١ "سلطات منح الشهادات الرقمية"(Certification Authorities):

لابد أن تصدر شهادة التعريف الرقمية عن سلطة معترف بها، وهي ما نطلق عليها " سلطة منح الشهادات الرقمية " (Certification Authority) كما ذكرنا، وهي هيئة تتحقق من الشخصية وتصدر شهادة التعريف اللازمة، ومن ثم فهي تقوم بخمس مهام:

١- استقبال طلبات الحصول على الشهادات.

٢- التأكد من شخصية الشخص أو المؤسسة مقدمة الطلب.

٣- إصدار الشهادة.

٤- إلغاء الشهادة.

٥- إتاحة معلومات عن الشهادات التي تصدرها لمن يطلب ذلك.

وقد يتم توزيع هذه المهام الخمس على أكثر من جهة، كأن تتولى جهة معينة التأكد من الشخصية لصالح سلطة منح الشهادات، كما يمكن لجهة أخرى أن تتولى عمليات إلغاء الشهادات، أو قد تتخصص جهة ما في تقديم المعلومات لمن يطلبها نيابة عن مجموعة من سلطات منح الشهادات الرقمية.

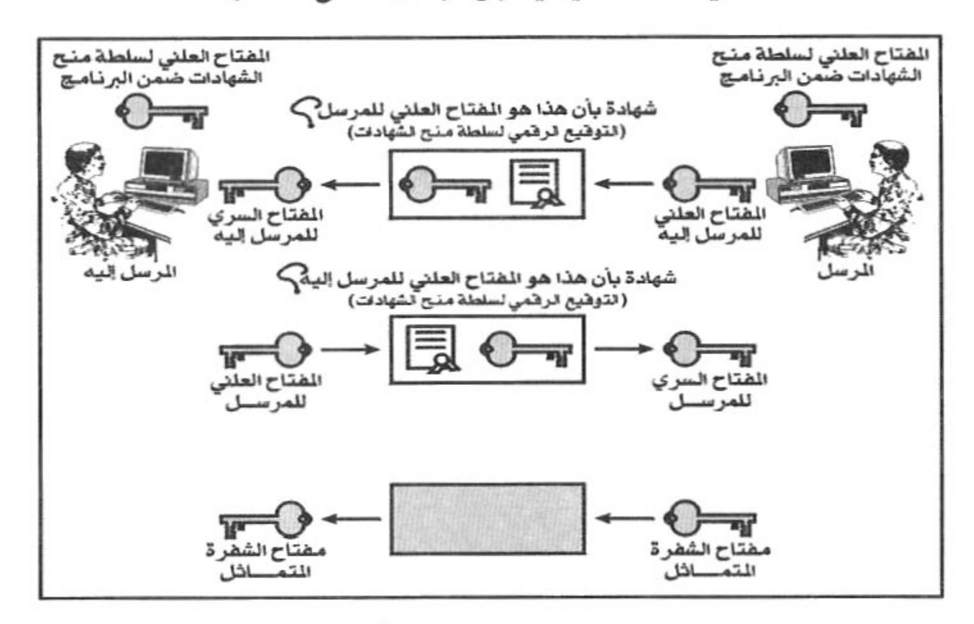
وتعتبر سلطات منح الشهادات الرقمية مكونًا هامًا من مكونات البنية الأساسية للمفتاح العام (PKI) كما أسلفنا.

وتتضمن شهادة التعريف الرقمية معلومات عن صاحب المفتاح، والجهة التابع لها، والمفتاح العلني له، ومدة صلاحية الشهادة، والتوقيع الرقمي على الشهادة، الذي يتم إعداده باستخدام المفتاح السري لسلطة منح الشهادات نفسها، مما يثبت صحة الشهادة وأنها صادرة عن هذه السلطة (لأن التوقيع الرقمي هنا هو توقيع سلطة منح الشهادات نفسها).

ولكي يمكن إتمام هذه العمليات بشكل آلي يوجد على الجهاز الخاص بكل مستفيد المفاتيح المختلفة لهذا المستفيد، والشهادة الرقمية التي تثبت شخصيته. كما أن المفاتيح العلنية لجميع سلطات منح الشهادات (CAs) الرئيسية موجودة ضمن جميع البرامج والتطبيقات التي تستخدم نظم التوقيع الرقمي، مما يسهل التأكد من شهادات التعريف الرقمية وصحة نسبتها إلى هذه السلطات. ويبين الشكل (٧-٩) كيفية تأكيد الشخصية بين الطرفين المتراسلين أولاً قبل تبادل مفاتيح الشفرة بينهما.

شكل (٧-٩)

تأكيد الشخصية يسبق تبادل مفتاح الشفرة



٧-٣-٢ استخدام سلطات منح الشهادات لتأكيد التوقيع الرقمي:

فيما يلي الخطوات اللازم اتباعها لإنشاء وتأكيد التوقيع الرقمي بواسطة سلطات منح شهادات التعريف الرقمية:

١- حصول الطرف المرسل من سلطة منح الشهادات على شهادة تعريف.

٢- يستخرج الطرف المرسل " رسالة مركزة " (Message digest) من الوثيقة المطلوب توقيعها، ثم يقوم بتشفير هذه الرسالة المركزة باستخدام رقمه السري لإنتاج " التوقيع الرقمي ".

٣- يرسل الطرف المرسل الرسالة والتوقيع الرقمي إلى المرسل إليه.

٤- يقوم المرسل إليه بالتأكد من أن المفتاح الذي وصله هو بالفعل مفتاح المرسل وذلك من خلال شهادة التعريف الخاصة بالمرسل.

٥- يقوم المرسل إليه بالتأكد من أن شهادة تعريف المرسل سارية المفعول ولم يتم إلغاؤها.

٦- يقوم المرسل إليه بفك شفرة التوقيع الرقمي باستخدام المفتاح العلني للمرسل لاستعادة الرسالة المركزة.

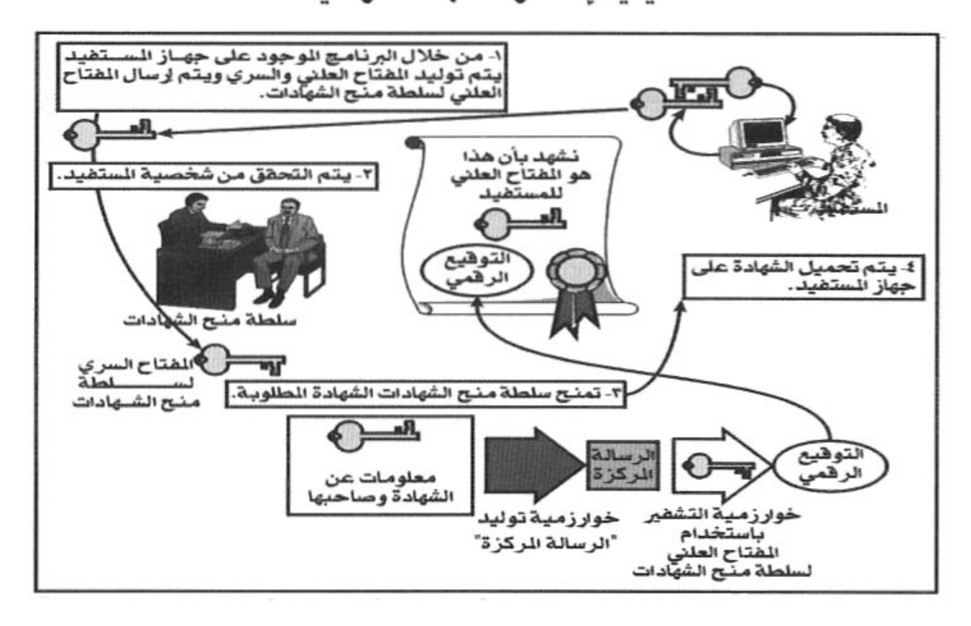
٧- يستخرج المرسل إليه " رسالة مركزة " أخرى من الوثيقة التي تسلمها، ويقارن هذه الرسالة المركزة بتلك التي استخرجها من التوقيع الرقمي.

٨- إذا تطابقت الرسالتان المركزتان فمعنى ذلك أن الوثيقة المستلمة هي نفسها الوثيقة التي تم إرسالها، وأن مرسلها هو فعلاً من يدعي ذلك.

وكما ذكرنا من قبل فكل هذه العمليات تقريبًا تتم آليًا، ويبين الشكل (٧-١٠) كيفية إصدار الشهادة الرقمية.

شكل (٧-١٠)

كيفية إصدار الشهادة الرقمية



٧-٣-٣ أشهر سلطات منح الشهادات الرقمية:

توجد عدة جهات مانحة للشهادات الرقمية (CAs) مثل:

(١) **شركة " بل ساين "** (BelSign): ويمكن الوصول إليها عن طريق موقعها على شبكة الإنترنت (www.belsign.com) وهي تمنح الشهادات للجهات وللأفراد على حد سواء، وبرغم أن هذه الجهة تختص أساساً بدول الاتحاد الأوروبي إلا أنها تقبل منح الشهادات لخارج دول أوروبا.

(٢) **شركة " فيري ساين " (VeriSign)**: وهي من أكبر الشركات مانحة الشهادات الرقمية، ولها نشاط ملحوظ في المملكة العربية السعودية، وهي تمنح جميع أنواع الشهادات، ويمكن الدخول على موقعها على الإنترنت (www.verisign.com) للحصول على الشهادات، ويمكن الحصول (مجانًا) على شهادة تعريف مدة صلاحيتها ٦٠ يومًا.

(٣) **شركة " ثوت "** (**Thawte**): والتي اشترتها شركة " فيري ساين " (Verisign) في عام ١٩٩٩، ويمكن الوصول إليها من خلال موقعها على شبكة الإنترنت (www.thawt.com)، وهي تمنح نوعين من الشهادات إحداهما للأفراد والأخرى لخوادم المواقع.

(٤) **شركة " بالتيمور "**(**Baltimore**): وهي شركة تقدم العديد من الخدمات، كما تقدم حلولاً للبنية الأساسية للمفتاح العلني (PKI)، كما تقدم هذه الشركة كذلك الكثير من الخدمات في مجال التجارة الإلكترونية وخاصة في مجال الأعمال (Business-to-Business) وأمن المؤسسات. ويمكن الوصول إلى موقعها على شبكة الإنترنت من خلال العنوان التالي: http://www.baltimore.com

(٥) **شركة إنترست** (**Entrust**): وهي شركة تقدم الشهادات الرقمية للخوادم لتأكيد شخصية المواقع على شبكة الإنترنت لضمان أمن المعاملات على الشبكة. ويمكن الوصول إلى موقعها على شبكة الإنترنت من خلال العنوان التالي:

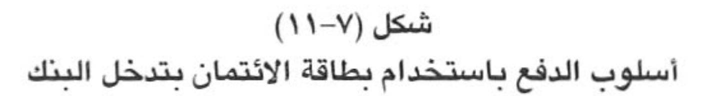
http://www.entrust.com

٧-٣-٤ الاستخدامات العملية للشهادات الرقمية:

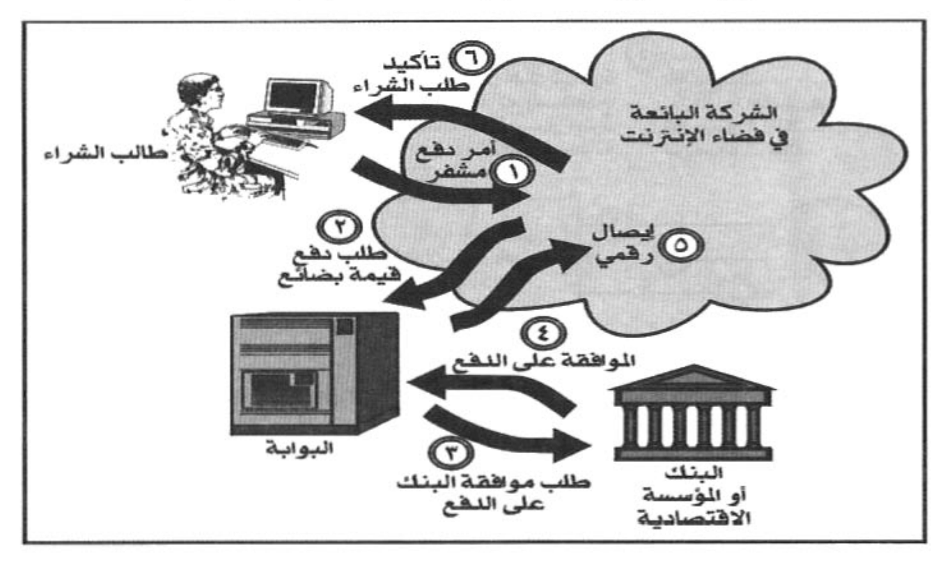
قد تلجأ بعض الجهات إلى استخدام الشهادات الرقمية لتعريف موظفيها، وذلك بهدف السماح لهم باستخدام التطبيقات الداخلية أو الدخول إلى قواعد البيانات في الشبكة الداخلية. وتستخدم هذه الجهات نوعًا آخر من الشهادات الرقمية أكثر قوة وأهمية وهي " شهادات الخوادم " (Server certificates) وهي التي تحتاج إليها المؤسسات لأعمالها الرسمية كإرسال طلبات أو التعاقد على صفقات ذات مبالغ كبيرة. وعندما يدخل أحد العملاء إلى موقع المؤسسة فإنه يحتاج إلى التأكد من أنه قد دخل بالفعل إلى الموقع المطلوب، وتؤدي الشهادة الممنوحة لخادم الموقع هذا الغرض.

الشركات التي تود ممارسة التجارة الإلكترونية عليها أن تحصل أولاً على شهادة رقمية للخادم الرئيسي في موقع الشركة، حتى تستطيع استقبال أرقام بطاقات الائتمان الخاصة بالعملاء في أمان، وإلا فإن الجهة المركزية التي ستشرف على عمليات التجارة الإلكترونية في المملكة (ولتكن وزارة التجارة مثلاً) لن تسمح لها بممارسة هذا النشاط. وتعتبر التجارة الإلكترونية هي أهم الاستخدامات العملية للشهادة الرقمية.

يتم حاليًا استخدام البنوك أو بعض المؤسسات الاقتصادية كطرف ثالث في عمليات التجارة الإلكترونية. ويبين الشكل (٧-١١) هذه العملية حيث يقوم طالب الشراء بتقديم " أمر دفع مشفر " (١) للشركة التي تقدم الخدمة أو السلعة عبر شبكة الإنترنت، فتقوم الشركة من جانبها بتقديم " طلب دفع قيمة بضائع " للبوابة (Gateway) (٢) التي تتولى التعامل مع البنك أو المؤسسة الاقتصادية، وتطلب " البوابة " موافقة البنك على الدفع (٣). وعند ورود موافقة البنك (٤) ترسل " البوابة " إيصالاً رقميًا إلى الشركة، (٥) وهنا تقوم الشركة بإرسال تأكيد طلب الشراء إلى طالب الشراء (٦) وتتم المعاملة المالية بهذا الشكل.



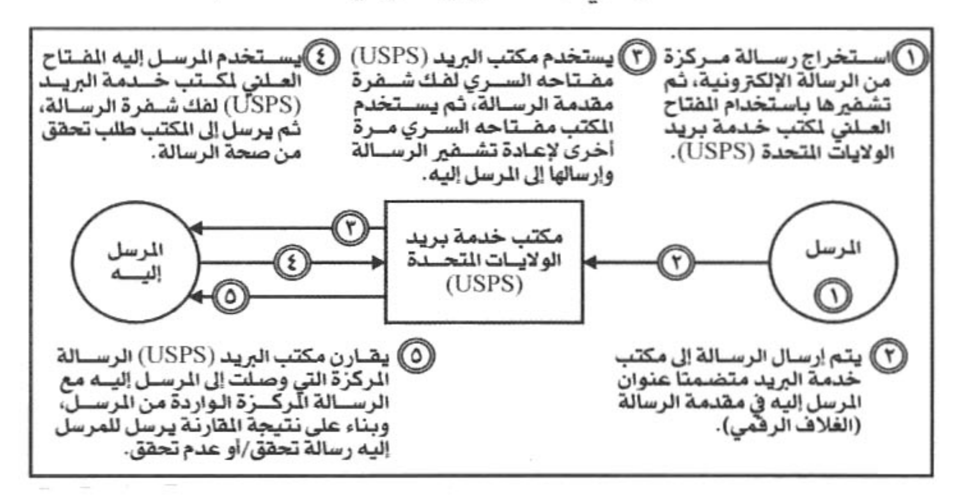
شكل (٧-١١)
أسلوب الدفع باستخدام بطاقة الائتمان بتدخل البنك



٧-٤ الأغلفة الرقمية:

رأينا كيف أنه يمكن باستخدام أسلوب التشفير باستخدام المفتاح العلني إنشاء نظم معلومات آمنة في بيئة غير آمنة مثل بيئة الإنترنت. نرى كذلك أجهزة الصرف الآلي المنتشرة في كل حي كمثال جيد لما حصلنا عليه من تقنية التشفير، ففي هذه الآلات توجد أموال سائلة لا يمكن صرفها إلا للأفراد الذين يثبتون شخصيتهم من خلال " رمز المستفيد " (PIN) أو(Personal Identification Number)، وهذا الرمز تتم حمايته عن طريق تشفيره بواسطة جهاز الصرف الآلي نفسه قبل إرساله من خلال الشبكة إلى بنك المستفيد، فإذا أكد البنك صحة رمز المستفيد استطاع المستفيد صرف المبلغ المطلوب.

شكل (٧-١٢)
الغلاف الرقمي (خدمة بريد الولايات المتحدة)



أحد التطبيقات الهامة للتوقيع الرقمي هو الغلاف الرقمي. اكتسب " الغلاف الرقمي " هذا الاسم لأنه يحتوي على عنوان المرسل إليه في مقدمة الرسالة الإلكترونية، تماماً كما يحدث في أغلفة رسائل البريد العادي. وأشهر الأمثلة على " الغلاف الرقمي " هو تطبيق " خدمة بريد الولايات المتحدة " (USPS) أو (United States Postal Service) حيث يتاح للعملاء الحصول على خاتم بريد إلكتروني رسمي يحدد الوقت والتاريخ، ويوضع هذا الخاتم على ملفات البريد المنقولة. كما يضمن سلامة الوثيقة خلال النقل بين المرسل ومكتب البريد الإلكتروني الافتراضي، وكذلك بين هذا المكتب والمرسل إليه. فإذا فشل الملف المنقول في اجتياز اختبار التدقيق، يقوم المكتب بإرسال رسالة تحذير للمرسل إليه بأن هناك احتمال وجود تلف في الرسالة أو حدوث محاولة اختراق لها. كما يقدم النظام إمكانية إرسال الخطابات المسجلة وإيصالات استلام البريد (بريد بعلم الوصول) لمن يشاء من العملاء.

يبين الشكل (٧-١٢) كيفية استخدام خدمة البريد لتكون همزة الوصل بين المرسل والمرسل إليه بحيث لا يحتاج أي منهما إلى الحصول على المفتاح العلني للطرف الآخر،

وإنما لا يحتاج المستفيد من هذه الخدمة إلا إلى معرفة المفتاح العلني لمكتب البريد (USPS)، ويتم التعامل وفقًا للخطوات الآتية المبينة في الشكل:

١- يقوم المرسل باستخراج " رسالة مركزة " (Hash) من الرسالة الإلكترونية المطلوب إرسالها، ثم يقوم بعد ذلك بتشفير هذه الرسالة المركزة باستخدام المفتاح العلني لمكتب خدمة بريد الولايات المتحدة (USPS).

٢- يتم إرسال الرسالة الموقعة رقميًا (الرسالة + الرسالة المركزة المشفرة) إلى مكتب خدمة البريد (USPS) متضمنة عنوان المرسل إليه في مقدمة الرسالة (Header) وهو ما نطلق عليه " الغلاف الرقمي ".

٣- يستخدم مكتب البريد (USPS) مفتاحه السري لفك شفرة مقدمة الرسالة ويتعرف على عنوان المرسل إليه، ثم يقوم المكتب بإعادة تشفير الرسالة باستخدام مفتاحه السري وإرسالها إلى المرسل إليه.

٤- يستخدم المرسل إليه المفتاح العلني لمكتب البريد (USPS) لفك شفرة الرسالة، ثم يرسل طلب تحقق من صحة الرسالة إلى مكتب البريد.

٥- يقارن مكتب البريد الرسالة المركزة التي وصلت إلى المرسل إليه مع الرسالة المركزة الواردة من المرسل، فإذا تطابقتا قام بإرسال رسالة تحقق إلى المرسل إليه ليطمئنه على سلامة الرسالة، وإذا لم تتطابقا أرسل رسالة تحذير إلى المرسل إليه.

٧-٥ الأجهزة والتقنيات الحديثة لمراقبة الشبكات:

يوجد في الأسواق في الوقت الحالي العديد من أجهزة وتقنيات مراقبة الشبكات تختلف في مهامها، وتختلف في كفاءتها، وتختلف في مجالات استخدامها. كما أن بعضها يصلح للاستخدام في الشبكات المحدودة، والبعض الآخر يصلح للشبكات الكبيرة، وسنستعرض في هذا القسم بعض هذه الأنواع من الأجهزة.

تنقسم أجهزة وتقنيات تأمين الشبكات إلى أربعة أقسام أساسية هي:

(١) **أجهـــزة وتقنيـــات تحـــديـــد الـــشخـصيـــة والـتحقق مـنهـــا (Identification and authentication)**: والتي تهدف إلى دعم الأساليب التي يستخدمها المستفيد للتحقق من الشخصية، وهذه الأجهزة إما أن تعتمد على شيء يكون في حوزة المستفيد مثل " البطاقات الذكية "(Smart cards)، أو تعتمد على شيء يعرفه المستفيد مثل كلمة سر، أو شيء لصيق بالمستفيد ولا ينفصل عنه مثل بصمة الإصبع.

(٢) **أجهزة وتقنيات مراقبة الاستخدام (Access Control)**: وتهدف هذه الأجهزة إلى معالجة قصور نظم التشغيل في هذا المجال. وتعتبر جدران الحماية (Firewalls) من بين هذه الأجهزة.

(٣) **أجهزة وتقنيات فحص النظم (Scanners)**: ومهمتها فحص بنية الشبكة للبحث عن الثغرات أو نقاط الضعف. وهي عادة تعمل على فترات مجدولة، ومعظم هذه الأجهزة يستطيع معالجة الثغرات التي تكتشفها في تهيئة أجهزة الشبكة. وهي وسيلة ممتازة للتأكد من أن السياسة الأمنية للمؤسسة مطبقة بشكل صحيح بواسطة العديد من الأجهزة الأمنية الموجودة بالموقع. ولو أن كثير من شركات أمن المعلومات في الوقت الحالي تعرض فاحصات النظم باعتبارها من أجهزة كشف الاقتحام (Intrusion detection products) باعتبار أن هذه الأجهزة تبحث عن نقاط الضعف التي يمكن أن تستغل بواسطة المهاجمين.

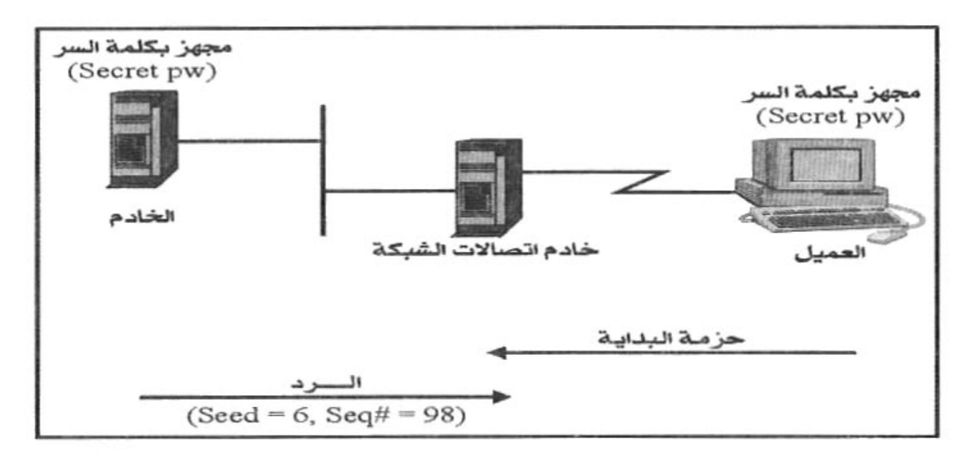
(٤) **أجهزة وتقنيات كشف الاقتحام والمراقبة(Intrusion detection and monitoring)** : مهمة هذه الأجهزة هي مراقبة النظم، وترقب أي محاولات اقتحام قد تحدث للشبكة. محاولات الاقتحام هذه قد تكون بسيطة لا تتعدى برنامجاً يحاول تعديل اسم مستفيد، أو قد تكون معقدة تحتوي على سلسلة من العمليات التي قد تتعدى النظام المطلوب حمايته إلى نظم أخرى. وهذه الأجهزة تستفيد كثيراً في أداء مهمتها من سجلات وقائع الاستخدام (System logs) والفرق الأساسي بين أجهزة كشف الاقتحام وفاحصات النظم أن هذه الأخيرة تعمل على فترات

(Off line) وليس بشكل مباشر، بينما الأولى تعمل بشكل مباشر (On line) وطوال الوقت.

٧-٥-١ أجهزة وتقنيات تحديد الشخصية والتحقق منها:
(Identification and authentication)

من أهم هذه التقنيات هي تقنيات تأمين كلمة السر، والأجهزة التي تستخدم كلمة السر مرة واحدة. وقد اخترنا من بينها نظام كلمة السر التي لا تتكرر(S/key)، وقد تم تصميمه لمواجهة الاقتحام الذي يتم بأسلوب إعادة الإرسال (Replay)، والذي تعرضنا له بالتفصيل في الفصل الخامس من هذا الكتاب (أساليب انتهاك شبكات المعلومات). وفي هذا النوع من أساليب الاقتحام يتم التنصت على الاتصالات الجارية عبر الشبكة حتى يمكن اقتناص اسم مستفيد وكلمة سر يمكن استخدامهما فيما بعد.

شكل (٧-١٣)
بدء عمل نظام (S/Key)

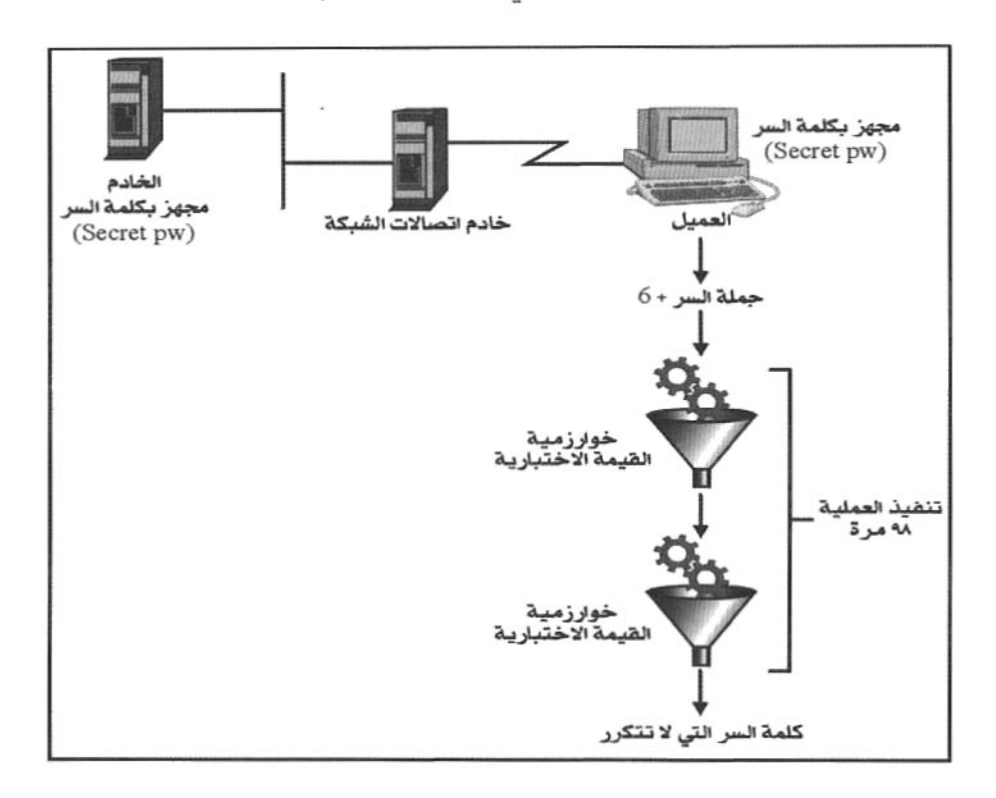


ويعتمد عمل نظام (S/key) على مشاركة " الخادم " و" العميل "، حيث يتم تزويد كل منهما في البداية بنفس " جملة المرور (Pass phrase) وعدد مرات إدخال البيانات

لخوارزميـة القيمة الاختبارية. ويبين شكل (٧-١٣) كيفية بدء عمل النظام، إذ يبدأ جهاز " العميل " بـإرسال حـزمة البـدايـة فيـرد " الخادم " بمعلـومتين: رقم مـسلسل(Seq #) ورقـم عشوائي (Seed)، ويتم اسـتخدامهما في استخـراج كلمة السـر التي لا تتكرر في ثلاث خطوات يبينها الشكل (٧-١٤):

شكل (٧-١٤)

حساب كلمة السر التي لا تتكرر بنظام (S/Key)



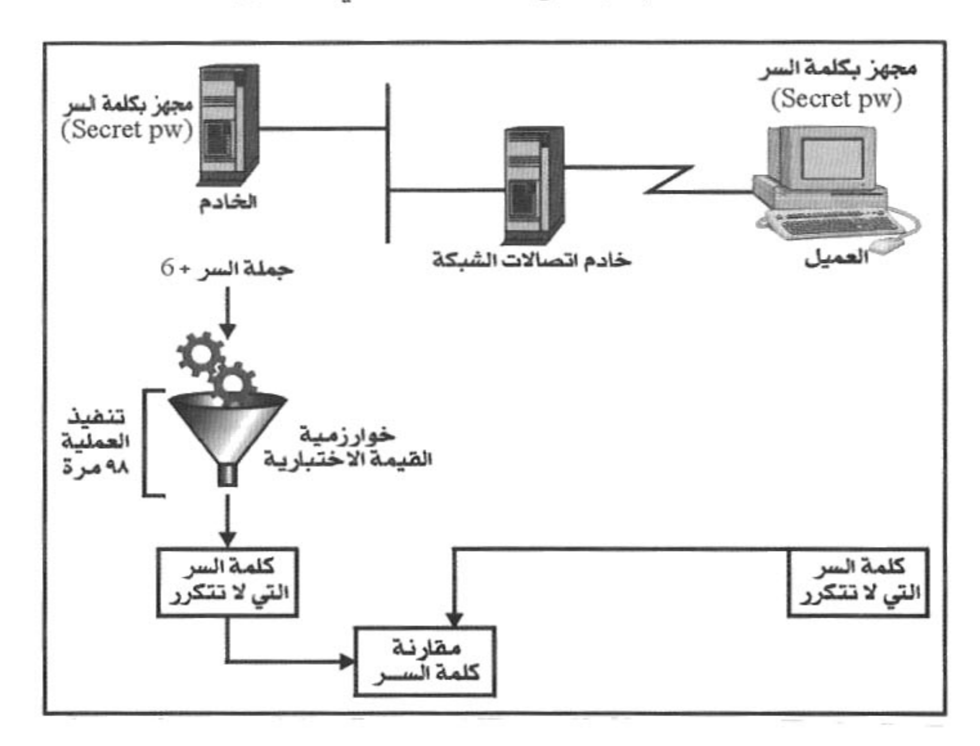
(١) الخـطوة التمهيـدية: حيث يـدخل " العميل " جملة المرور، ثم يتم إضافـة هذه الجملة إلى الرقم العشوائي (Seed) الذي تم إرساله (غير مشفر) من " الخـادم ".

(٢) خطوة التوليد: حيث يتم تنفيذ خوارزمية القيمة الاختبارية (Hash) عدة مرات على هذه الجملة لإنتاج كلمة سر ذات ٦٤ خانة (Bit)، وهذا العدد من المرات هو الرقم المخزن في كل من جهاز " العميل " وجهاز " الخادم ".

(٣) خطوة العرض: التي تأخذ كلمة السر المنتجة في الخطوة السابقة وتعرضها في صورة مقروءة.

في المرحلة النهائية المبينة في شكل (٧-١٥) يقوم " العميل " بإرسال كلمة السر التي لا تتكرر إلى " الخادم " حيث تتم مراجعتها والتأكد من صحتها.

شكل (٧-١٥)
" الخادم " يراجع كلمة السر التي لا تتكرر



٧-٥-٢ أجهزة وتقنيات التحكم في السماح بالاستخدام (Access Control):

هذه التقنيات قد تصنف أحيانًا تبعًا لتقنيات تحديد الشخصية والتحقق منها، ولكن الكثير من المراجع تصنفها بشكل مستقل [Kaeo ١٩٩٩] ومن هذه التقنيات (TACACS+) و (RADIUS) و(Kerberos) و(DCE) و(FORTEZZA). وكثيرًا ما تستخدم التقنيتان (TACACS+) و (RADIUS) معًا للتحكم في السماح بالاستخدام من جانب المتصلين عن بعد من خلال خطوط المراقمة (Dial-up). ويعتمد نظام (TACACS+) على الفصل الكامل بين العمليات الثلاث " التأكد من الشخصية " (Authentication)، و" السماح بالاستخدام "(Authorization)، و" تسجيل وقائع الاستخدام " (Accounting).

أما نظام خدمة الاتصال عن بعد " راديوس " (RADIUS) أو (Remote Address Dial-In User Service) فيستخدم بروتوكول " بيانات المستفيد " (UDP) في نقل البيانات، وهو يعتمد على نظام " الخادم/العميل " ويتولى تنفيذ العمليات الثلاث (التأكد من الشخصية، والسماح بالاستخدام، وتسجيل وقائع الاستخدام).

أما بروتوكول (Kerberos) فيستخدم عادة في الجامعات ليقوم أولاً بالتأكد من شخصية المستفيدين ومن أن الخدمات التي يحصلون عليها من الشبكة هي نفس الخدمات المصرح لهم بها. وبعد ذلك يحدد مستوى الصلاحية لكل مستفيد.

أما نظام (DCE) أو (Distributed Computing Environment) ونظام (FORTEZZA) فهما غير واسعي الانتشار.

جدران الحماية (Firewalls) تعتبر هي أيضًا من الأجهزة المستخدمة في التحكم في السماح بالاستخدام وسنفرد لها فصلاً خاصًا في هذا الكتاب وهو الفصل التاسع.

٧-٥-٣ أجهزة وتقنيات فحص النظم (Scanners):

تعرضنا في الفصلين السابقين (الخامس والسادس) لهذا النوع من الأجهزة التي تتولى

(دوريًا) فحص مكونات الشبكة وأجهزة أمن المعلومات بها، ومراجعة تهيئتها (Configuration) للتأكد من عدم وجود ثغرات أمنية تسمح بمهاجمة الموقع. ومن المهم أن نوضح أن هذه الأجهزة لا تراقب الرسائل المارة بالشبكة، ولا تعمل بشكل مباشر(On line)

تقوم هذه الأجهزة خلال الفحص الدوري بمراجعة الاحتمالات التالية:

- وجود نسخ قديمة من البرمجيات معروف أن بها ثغرات.
- وجود خطأ في التهيئة ناتج عن تركيب الجهاز كما هو بما فيه من اختيارات افتراضية قد تشكل ثغرات أمنية.
- وجود خطأ في تهيئة نظام التشغيل أو في تركيب بعض البرمجيات.
- وجود بعض برامج الفيروسات التي قد تكون مزروعة في النظام.

وبعض هذه الأجهزة الفاحصة يعمل مع نظم التشغيل " يونكس " وبعضها مع نظم " وندوز إن تي ".

ينقسم هذا النوع إلى فاحصات عن بعد (Remote scanners) وفاحصات محلية (Local scanners)

٧-٥-٢-١ " الفاحصات عن بعد "(Remote scanners):

تقوم هذه الفاحصات بفحص الشبكة، وتكتشف إذا كان النظام مثلاً يسمح للغرباء باستخدام خدمة نقل الملفات وتحميل الملفات على خادم الموقع، فإن ذلك يفتح الباب للمقتحمين لاستخدام الموقع كمركز لتوزيع البرامج المسروقة. كما يستطيع " الفاحص عن بعد " اكتشاف إذا ما كانت الخدمات المقدمة على الشبكة تقوم بتسريب بعض المعلومات عن المستفيدين أو تسمح للمقتحمين بالوصول إلى بيانات النظام.

من خلال إرسال حزم بيانات اختبارية عن بعد يستطيع هذا النوع من الفاحصات اكتشاف مدى ضعف مقاومة الخدمات المقدمة على الشبكة. ويستطيع كذلك اكتشاف عيوب تهيئة جدران الحماية وخادم الشبكة.

٧-٥-٣-٢ " الفاحصات المحلية "(Local scanners):

تستطيع هذه الفاحصات أن تجوس خلال الملفات بحثًا عن أخطاء التهيئة (Configuration errors) أو التعديلات التي قد يكون أحد المهاجمين قد أدخلها على هذه الملفات. كما تستطيع التأكد من أن السياسة الأمنية الموضوعة مطبقة بالفعل من خلال تهيئة جدار الحماية أو خادم البروكسي. يتميز الفاحص المحلي عن الفاحص عن بعد بأنه يعمل على الشبكة موضوع الفحص مباشرة ومن ثم يستطيع اكتشاف مشكلات ليس في مقدور الفاحص عن بعد اكتشافها، مثل القابلية للتعرض لهجوم الإغراق بالبيانات (Buffer overflow) وهو ما لا يستطيعه الفاحص عن بعد إلا إذا قام باختراق الشبكة! كما يقوم هذا النوع بالتأكد من مستوى التعديلات التي تم إدخالها على النظام وهل هي أحدث التعديلات أم لا.

وهكذا فمن المفضل استخدام الاثنين معًا (الفاحصات المحلية والفاحصات عن بعد)، فعمل كل منهما مكمل للآخر.

ويوجد الآن في الأسواق العديد من هذه الأدوات، منها (COPS) الذي أنتجه الباحثون في جامعة " بوردو " ، وهناك أيضًا (SAFESuite) وهو نظام لأمن الإنترنت (ISS) أو (Internet Security System) والذي انتشر استخدامه في هذه الأيام.

وفاحصات أمن الإنترنت (ISS) تأتي الآن على نوعين: إما " فاحصات أمن النظام " (S٣) أو(System Security Scanners) أو" فاحصات الإنترنت " (Internet scanners) – فأما فاحصات أمن النظام (S٣) فهي تمتاز بتنوع تهيئتها وكفاءة التقارير المخرجة منها والعدد الكبير من الثغرات ونقاط الضعف التي تستطيع اكتشافها، بينما تبحث فاحصات الإنترنت بصفة أساسية عن الثغرات الموجودة في الشبكة وفي خادم الشبكة وجدار الحماية.

٧-٥-٤ أجهزة وتقنيات كشف الاقتحام والمراقبة:
(Intrusion detection and monitoring)

في الفصل القادم " نظم كشف عمليات الاقتحام " سنتحدث بالتفصيل عن هذا النوع من الأجهزة الذي يتم تركيبه في الشبكة بحيث يترقب أي محاولة اقتحام ويكتشفها ويبلغ عنها ويحاول إبطال مفعولها. وسنعرض هنا باختصار لأشهر أنواع هذه الأجهزة المتوافرة بالأسواق.

(١) (RealSecure): وهو من أكثر نظم كشف الاقتحام انتشارًا [Northcutt ١٩٩٩] وهو، شأنه شأن جميع نظم كشف الاقتحام، ليس مثاليًا. فهو قادر على اكتشاف " بصمات الاقتحام " (Intrusion signatures) (أى علاماته ودلائله) التي تتم تغذيته بها فقط. وهو نظام سهل الاستخدام، ويستطيع المستفيد تحسين أدائه ومعالجة عيوبه، وهذه ميزة هامة تحسب له؛ فكلما تمت تغذيته بالمزيد من " بصمات الاقتحام " ازدادت كفاءته. وقد أضيف إلى النظام في نسخته الأخيرة إمكانيات تحليل الاتجاهات وقاعدة بيانات واسعة. وجدير بالذكر أن هذا النظام يعمل في بيئة " وندوز إن تي ".

(٢) (NetProwler): هذا النظام يعمل في بيئة " وندوز إن تي "، وإن كان غير واسع الانتشار.

(٣) (NFR) أو (Network Flight Recorder) والذي يعمل في بيئة " يونكس "، وهذا النظام يمكن أن يصبح عظيم الفائدة إذا تم استخدامه بواسطة خبير، فهو جهاز مراقبة عام للشبكات ويتطلب من المستخدم خبرة ببيئة " يونكس ". وهو نظام قادر على اكتشاف كثير من أساليب الاقتحام.

(٤) (Net Ranger) هذا النظام من إنتاج شركة " سيسكو " (Cisco)، وهو نظام آخر يعمل في بيئة " يونكس "، ومن مزاياه تكامله مع الموجهات (Routers)التي تنتجها شركة " سيسكو "، ومن عيوبه تكلفته العالية. ويمكن تهيئة هذا النظام لاكتشاف أحداث معينة والإبلاغ عنها، ولذلك تسميه الشركة المنتجة (Dynamic security component).

٧-٥-٥ تقنية " الخصوصية الفائقة "(PGP) لحماية البريد الإلكتروني:

لابد من أن تستخدم المؤسسات المختلفة تقنيات قوية لتضمن أمن معلوماتها المتداولة في شبكة الإنترنت، ولتستطيع إقناع عملائها باستخدام بطاقات الائتمان الخاصة بهم في اتصالاتهم معها. وإحدى التقنيات المتداولة حاليًا هي تقنية " الخصوصية الفائقة " (PGP) أو (Pretty Good Privacy) والتي طورها في البداية " فيليب زيمرمان "، وهي إحدى تقنيات حماية البريد الإلكتروني. وتعتمد النسخ القديمة منها على تقنية(RSA) التي شرحنا استخدامها في بداية هذا الفصل. ويمكن للقارئ الحصول على نسخة مجانية منها (للاستخدام غير التجاري) من موقع شركة (Network associates) على العنوان التالي:

http://www.nai.com/default _ pgp.asp

وعلى هذا الموقع ستجد نظام (PGP) في صورة المصدر (Source code) وهذه الصورة مخصصة لنظم " يونكس " وستجده في الصورة القابلة للتنفيذ (Executable code) وهي الصورة المخصصة للعديد من نظم التشغيل الأخرى بما فيها " ويندوز "، " دوس "، " ماكنتوش ". وتتمتع هذه التقنية بواجهة مستفيد ممتازة (لنظام وندوز ونظام ماكنتوش فقط).

وهذه التقنية هي الأفضل فيما يخص البريد الإلكتروني، حيث يمكنك من خلالها تشفير رسائلك قبل إرسالها عبر الشبكة، كما أنك تستطيع من خلالها استخدام التوقيعات الرقمية (Digital signatures) لإثبات صدور الرسالة منك.

تتضمن تقنية (PGP) في نظم " وندوز " المختلفة المكونات التالية:

١- PGP key management: وهو المكون الذي يتعامل مع المفاتيح السرية والعلنية الخاصة بك وبالآخرين ممن تتصل بهم.

٢- PGPnet (VPN): ويستخدم لإنشاء الشبكة الخاصة الافتراضية.

٣- PGP Eudora plugin: ويستخدم في حالة اعتمادك على نظام (Eudora) للبريد الإلكتروني.

٤- PGP M.S Exchange/Outlook plugin: ويستخدم في حالة اعتمادك على نظام البريد الإلكتروني (MS Exchange) أو (MS Outlook)

٥- PGP MS Outlook express plugin ويستخدم في حالة اعتمادك على نظام البريد الإلكتروني (MS Outlook express)

٦- PGP command line ويستخدم عند الحاجة إلى إدخال الأوامر من سطر الأوامر بدلاً من الواجهة الرسومية.

٧- PGP user's guide ويستخدم لشرح استخدام النظام.

ذكرنا أن النسخ القديمة من هذه التقنية تستخدم تقنية (RSA)، أما النسخ الحديثة منها (النسخة ٥,٠ وما بعدها) فهي تستخدم بالإضافة إلى تقنية (RSA) تقنية (Diffie-Hellman/Dss) وهي أيضًا من تقنيات التشفير باستخدام المفتاح العلني. يمكن للمستفيد الاختيار من بين التقنيتين وفقًا لما هو متاح لدى الأطراف الأخرى التي يتبادل معها الرسائل. والتقنية الثانية " ديفي - هيلمان " أفضل، ما لم يكن هناك الكثير ممن تتبادل معهم الرسائل والذين يستخدمون التقنية الأخرى. ويقوم الكثير من المستفيدين بإعداد مفتاحين للتشفير، كل واحد منهما يعتمد على إحدى التقنيتين، ويستخدمون أيًا منهما وفقًا لمقتضيات الأمور.

يستطيع المستفيد عند إعداد مفتاحه (مفتاحان في الحقيقة، واحد سري والآخر علني) أن يحدد أن هذا المفتاح مفتاح دائم، أي ليست له مدة صلاحية معينة، وهذا يناسب استخدام الأفراد. بينما إذا كان المفتاح يخص مجموعة تعمل في مشروع معين، فيمكن تحديد موعد معين لانتهاء صلاحية المفتاح، وبعد هذا التاريخ لا يمكن استخدام المفتاح في التشفير.

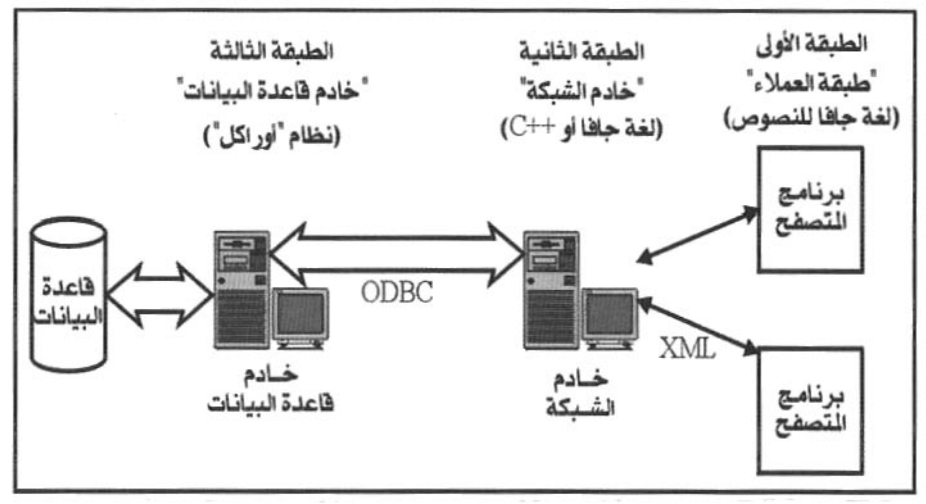
٧-٥-٦ بنية الطبقات الثلاث (Three-tier structure):

من بين التقنيات المستخدمة لحماية الشبكات تقسيم الشبكة إلى عدة طبقات منفصلة

عن بعضها، ويبدو ذلك جليًا في " بنية الطبقات الثلاث " (Three-tier structure)، والتي تشتمل على طبقة " العملاء " (Clients) والتي تتصل بالشبكة من خلال الحاسبات الشخصية، وطبقة " خادم الشبكة " (Web server)، وطبقة " خادم قاعدة البيانات " (Database server) وتشتمل على الخادم الذي يتولى التعامل مع قاعدة البيانات. هذا الفصل بين الطبقات يعتبر أحد أساليب الحماية كما يبين شكل (٧-١٦).

شكل (٧-١٦)

بنية الطبقات الثلاث للاتصال بالشبكة



تشتمل الطبقة الأولى " طبقة العملاء " على برنامج " المتصفح " (Browser)الذي يتولى مهمة عرض الصفحات التي يتم الحصول عليها، إما من خادم الشبكة أو من خادم قاعدة البيانات، ويمكن استخدام لغة " جافا للنصوص " (Java script) في هذه الطبقة. والطبقة الثانية " طبقة خادم الشبكة " تحتوي على الخادم الذي يتولى معالجة صفحات النسيج (Web pages)، وفي هذه الطبقة يمكن استخدام لغة " جافا " أو لغة (C++) والطبقة الثالثة " طبقة خادم قاعدة البيانات " وهي تحتوي على الخادم الذي يتولى التعامل مع قاعدة البيانات، ويمكن استخدام برمجيات " أوراكل " عليه.

يتم الربط بين هذه الطبقات وبعضها، فمثلاً يمكن الربط بين طبقة العملاء وطبقة خادم الشبكة باستخدام " لغة العلامات الممتدة " (XML) أو (Extended Markup Language)، كما يتم الربط بين خادم الشبكة وخادم قاعدة البيانات باستخدام " الاتصال الشيئي بقواعد البيانات " (ODBC) أو (Object Database Connectivity) [غنيمي ٢٠٠١].

يلاحظ من الشكل (٧-١٦) أن العملاء لا يستطيعون التعامل مباشرة مع قاعدة البيانات أو حتى خادم قاعدة البيانات وهذا الفصل في صالح الحماية.

في الفصل القادم سوف نتعرض بالتفصيل لأحد أهم تقنيات الحماية وهي نظم كشف عمليات الاقتحام (Intrusion detection systems).

الفصل الثامن
نظم كشف الاقتحام

بعد أن عالجنا في الفصل السابق التقنيات المختلفة المستخدمة لحماية الشبكات، فإننا نتناول في الفصول الثلاثة التالية بتفصيل أكبر ثلاثة من أهم هذه التقنيات في عالم أمن الشبكات: وهي نظم كشف الاقتحام، وجدران الحماية، والشبكات الخاصة الافتراضية.

نتناول في هذا الفصل نظم كشف الاقتحام (IDS) أو (Intrusion Detection Systems) فنبدأ بشرح طبيعة عمل هذه النظم، ثم نصنف في القسم الثاني أساليب الاقتحام المختلفة وفقًا للهدف منها. فنتحدث عن عرقلة الخدمة، والحصول على صلاحيات غير مرخص بها.

ثم ننتقل في القسم الثالث من هذا الفصل إلى الإجراءات المتبعة لتطبيق هذه النظم فنتحدث عن المواصفات التي يجب أن تتوفر في هذه النظم، وأساليب خداعها من إنذار كاذب بالاقتحام، إلى اقتحام لا يصحبه إنذار، إلى استبدال البرنامج. ونقدم المواصفات التي يجب أن تتمتع بها الأجهزة المستخدمة في هذه النظم.

في القسم الرابع نعرض بعض نظم كشف الاقتحام الحديثة المتوفرة في الأسواق في الوقت الحالي ونقيمها ونوضح المجال المناسب لاستخدامها. ونخصص القسم الخامس من هذا الفصل لموضوع تحليل عمليات الاقتحام الذي يتلو حدوث هذه العمليات.

ثم نقدم في القسم السادس بعض " السيناريوهات " لعمليات اقتحام فعلية وتحليلها ثم نختم هذا الفصل بالحديث عن نوع آخر من نظم كشف الاقتحام وهو " الأجهزة " (Hardware) المستخدمة في هذا المجال، وأهمية تعدد خطوط الدفاع في الشبكة المطلوب حمايتها.

٨-١ طبيعة عمل نظم كشف الاقتحام (IDS):

أصبحت نظم كشف الاقتحام (IDS) أو (Intrusion Detection Systems) في

الوقت الحالي من الأدوات التي لا تستغني عنها أي مؤسسة أو شركة لديها شبكة معلومات، خاصة إذا كانت هذه الشبكة مرتبطة بالإنترنت (وهي دائمًا كذلك)، هذا برغم أن هذه النظم تعتبر من التقنيات الحديثة جدًا. ونتوقع أن تلقى هذه التقنية الكثير من التطوير في السنوات القليلة القادمة. ولكن ما يجب أن نؤكد عليه أن هذه النظم ليست بديلاً عن جدران الحماية، وإنما هي مكملة لها لتشكيل منظومة الأمن الشاملة.

ولكن ما هي طبيعة هذه النظم وكيف تعمل؟ إن هذه النظم تراقب الرسائل المارة بالشبكة وتختبر كافة الحزم للتأكد من عدم مرور حزم مشبوهة، وفي حالة وجود مثل هذه الحزم يتم إيقافها والإعلان عنها. وهذه النظم مسلحة بالكثير من المعلومات عن أساليب الاقتحام المختلفة، بل إن بعضها يضم في قاعدة بياناته معلومات عن أكثر من ١٠٠ أسلوب اقتحام.

وعند الحديث عن نظم وأجهزة كشف الاقتحام (IDS) لا يجب أن نغفل أجهزة مسح الشبكة (Scanners)، والتي تتولى فحص الشبكة بحثًا عن نقاط الضعف التي يمكن أن ينفذ منها المهاجمون. وهذه الأجهزة لا تعمل طوال الوقت وإنما من وقت لآخر، فمثلاً عند تغيير تهيئة خادم الشبكة وللتأكد من أن هذا التغيير لم يخلق ثغرة أمنية، يتم تشغيل ماسح الشبكة (Scanner) لقراءة محتويات ملفات التهيئة والبحث عن أي شيء في هذه الملفات قد يستغل من قبل المهاجمين، وفي بعض الماسحات المتقدمة يقوم ماسح الشبكة بتعديل ملف التهيئة لعلاج المشكلة. وكما ذكرنا فبينما تعمل أجهزة كشف الاقتحام طوال الوقت لمراقبة الشبكة، فإن الماسحات تعمل على فترات عندما نحتاج إلى فحص الشبكة بحثًا عن الثغرات الأمنية [Escamilla ١٩٩٨]

وتتكون نظم كشف الاقتحام من جزأين: " الآلة " (Engine) وهي الجزء المسئول عن فحص وتحليل كل الرسائل المارة، و " أداة المراقبة " (Console) وهي التي يقوم مسئول الأمن من خلالها بإدارة " الآلة "، كما يتم من خلالها إصدار كافة التقارير الأمنية المطلوبة.

٨ـ٢ أساليب الاقتحام المختلفة:

يمكننا أن نصنف أساليب الاقتحام في مجموعات وفقًا لاعتبارات مختلفة، فيمكننا مثلاً أن نأخذ في الاعتبار مصدر الاقتحام كعامل مهم للغاية. فكلما كان المقتحم قريبًا من النظام كان خطره أعظم، وبالتالي فالمقتحم من الداخل يكون أكثر خطورة من شخص يقتحم النظام عن بعد (من خلال الإنترنت). ومن جهة أخرى فالمقتحم من الداخل يسهل التعامل معه عند اكتشافه ويمكن اتخاذ الإجراءات اللازمة في حقه، أما المقتحم من الخارج فهو طير طليق يصعب التعامل معه أو الوصول إليه. قبل انتشار استخدام الإنترنت كانت معظم عمليات الاقتحام تتم من الداخل، ولكن الصورة تغيرت بعد ظهور الإنترنت كوسيلة اقتحام ممتازة. فيمكننا أن نصنف أنواع الاقتحام إلى اقتحام من الداخل واقتحام من الخارج. ولكننا سنصنف أنواع الاقتحام حسب الضرر الذي يسببه كل نوع، فنصنفها إلى نوعين رئيسيين:

- أولهما: " عرقلة الخدمة " (DoS) أو(Denial of Service)
- والثاني: وهو الأخطر " الحصول على صلاحيات غير مرخص بها " ومن خلال هذا الأخير يمكن ارتكاب العديد من الجرائم.

٨ـ٢ـ١ عرقلة الخدمة (Denial of Service):

سمعنا مؤخرًا عن العديد من نظم (Windows NT)التي تعرضت لهجوم من الداخل تسبب في عرقلة الخدمة (Denial of Service) وتم ذلك بإرسال أنواع معينة من حزم الرسائل (UDP) تتسبب في تعطل النظام عن العمل. وهذا النوع يتم عادة من الداخل لأنه من المعتاد أن يتم حجب حزم الرسائل من نوع (UDP) بواسطة الموجهات الحاجبة (Screening routers) أو جدران الحماية (Firewalls)، لذلك فإن احتمال تسرب هذا النوع من الحزم من خارج الشبكة هو احتمال ضئيل. ويمكن أن يقوم المهاجم بالتسبب في عرقلة الخدمة بعدة طرق:

- استهلاك كل المساحة المخصصة لخادم الشبكة على القرص الثابت، أو تلك

المخصصة لفهرس (/tmp) الخاص بنظام " يونكس" (UNIX) لإبطاء النظام، أو إيقافه تمامًا عن العمل في بعض نسخ نظام " يونكس ".

- كتابة برنامج يقوم باستهلاك كل موارد النظام المتاحة مثل مساحات الذاكرة الوسيطة (Memory buffers)المخصصة لمنافذ الخدمات (Sockets) التي يقدمها خادم الشبكة.
- إغراق قائمة انتظار الطباعة بطلبات الطباعة الوهمية حتى لا يقبل النظام ملفات جديدة للطباعة.

تنفيذ مجموعة من البرامج في وقت واحد بحيث تكون مليئة بعمليات الإدخال والإخراج (I/O bound)

- في حالة استطاعة المهاجم الوصول إلى قوائم المستخدمين (ليس من الضروري الوصول إلى كلمات السر) فهو يستطيع إغلاق جميع حسابات المستخدمين عن طريق محاولة الدخول باسم كل منهم باستخدام كلمة مرور خاطئة عددًا من المرات يتجاوز عدد مرات الخطأ المسموح بها، فيغلق النظام الحساب. وهذا الأمر يمكن تنفيذه من الخارج كذلك بواسطة أي شخص يعرف أسماء المستخدمين، وهي قائمة لا يوجد حظر عليها.
- اعتمادًا على أن التطبيقات القديمة لا تقوم بعمليات التحقق من شخصية مرسل حزم الرسائل يمكن إقحام عنوان (IP address) مزيف وحزم رسائل مزيفة تتمكن من التسلل من خلال هذه التطبيقات القديمة، وتزداد سهولة تنفيذ هذا النوع من الهجوم إذا كان خادم الشبكة مصممًا بحيث يقبل الاتصال من أي نقطة (Node) داخل الشبكة.
- يمكن أن يكتب شخص ما برنامجًا يقوم بتوليد عدد كبير من معاملات (HTTP) تستهدف خادم النسيج (Web server) في الشبكة، ومعظم هذه الأجهزة ليست مهيأة لكي تكتشف أو تقاوم هذا النوع من الهجوم، ولن يفيد جدار الحماية أو الموجه الحاجب كثيرًا في هذا المجال لصعوبة تحديد قاعدة (Packet Filtering Rule) لحجب هذه

الأنواع، فما يحدث عادة هو أن خادم النسيج (Web server) في حالة ورود حزم رسائل كثيرة من نفس المصدر وفي نفس التوقيت فإنه سوف يقوم بحجب هذا المصدر. ولكن المهاجمين أذكى من ذلك فهم يقومون بتغيير عنوان مصدر الرسالة (IP address) باستمرار لتجنب الاكتشاف.

وقد بدأت نظم " يونكس " الحديثة اتخاذ بعض الاحتياطات التي تمنع هذه الأنواع من الهجوم بوضع قيود على صلاحيات المستخدمين فتمنعهم من استخدام مساحة كبيرة من القرص الصلب (في ملفات حساسة مثل tmp/) وتمنعهم من استخدام مساحات كبيرة في الذاكرة، وتضع قيودًا على عدد الملفات التي يسمح للمستفيد بفتحها آنيًا، والعمليات التي يسمح له بتنفيذها آنيًا، إلى جانب القيود على الموارد التي يشترك فيها كل المستخدمين. ولكن هذه الاحتياطات تتم في مواجهة المستخدمين المعرفين في قوائم الاستخدام، أما المتصلون من الخارج فيمكنهم انتحال شخصية مدير الشبكة (ومن ثم صلاحياته) التي عادة تكون أكبر وأوسع، والبعض يجعلها بغير حدود!!.

٨-٢-٢ الحصول على صلاحيات غير مرخص بها:

عند الدخول إلى نظام ما يكون للداخل إلى هذا النظام (سواء من داخل الشبكة أو من خارجها) صلاحيات محددة وفقًا لطبيعة عمله. فإذا أراد المقتحم الحصول على صلاحيات أعلى؛ فإنه يلجأ إلى وسائل تعتمد على ثغرات نظم التشغيل. تسمح نظم " يونكس" (UNIX) و" إن تي" (NT) للمستخدمين بالحصول على صلاحيات أعلى من خلال تشغيل بعض البرامج، خاصة إذا كانت هذه النظم تستخدم رموز الاستخدام الخاصة بالمجموعات (Group UIDs) وسوف نتعرض لها عند تقييمنا لأمن نظم التشغيل في الفصل الثاني عشر. ويمكن اختراق البرامج ذات الصلاحيات العالية (Privileged Programs) بوسائل عديدة منها:

- إغراق المساحات الوسيطة للبرنامج (Buffers) بالبيانات، باستغلال حقيقة أن هذه

البرامج لا تختبر عادة أحجام البيانات المدخلة لها.

- استغلال عدم قيام هذه البرامج بفحص المعاملات المدخلة فيمكن إدخال بعض الأوامر على أنها معاملات؛ فيقوم البرنامج بتنفيذها مثل (test.cgi hack) !!!. ومن ثم يتم تنفيذ برنامج معين (اسمه hack مثلاً) يؤدي ما يشاء من تخريب دون أن يمنعه النظام.
- جعل البرنامج يتعامل مع مورد مختلف عن المورد الذي صمم من أجل التعامل معه، كأن يتم خداع البرنامج لكي يقوم بتنفيذ برامج مدسوسة بدلاً من تنفيذ البرامج المعتادة.
- استغلال فرصة أن البرنامج لا يعرف مسار (Path) الملفات التي يتعامل معها بشكل كامل فيمكن خداعه بجعله يتعامل مع ملفات أخرى غير الملفات الحقيقية.

للأسف فإن معظم نظم التشغيل المتاحة في الأسواق ملأى بهذه الأنواع من الثغرات.

كما يمكن لشخص من الخارج أن يخترق النظام عن طريق:

- الدخول على البرامج التي لا تسمح بالدخول من الخارج عن طريق إيهام البرنامج أن المتصل هو إحدى الشبكات الداخلية أو خادم النسيج (Web server) في الشبكة. ويفسح المجال لهذا الاختراق عدم اتخاذ الاحتياطات الكافية عند برمجة خادم النسيج. بل إن بعض المهاجمين يمكنهم استغلال هذه الثغرة في زرع بعض الفيروسات أو برامج حصان طرواده (Trojan horse) في بعض الفهارس التي يلجأ إليها المستخدمون الآخرون عادة للحصول على ما بها من ملفات. ويقومون بعد الحصول على الصلاحيات الكافية بزرع هذه البرامج الملوثة في تلك الفهارس، وعند قيام مستفيدين آخرين بطلب محتويات الفهرس يحصلون (دون أن يدروا) على هذه الملفات التي تخرب نظمهم.
- الدخول إلى النظام (Iogin) مخترقًا قواعد تحديد الشخصية المستخدمة، ويتم ذلك

عن طريق مراقبة المتصلين الآخرين عن بعد، وعند رصد دخول شخص ذي صلاحيات عالية (Supervisor) إلى النظام من خلال بروتوكول غير محمي ضد زرع حزم الرسائل أو ضد اعتراض البث (Session hijacking)، عند رصد هذا الدخول يستطيع المهاجم اختراق النظام مستخدمًا الصلاحيات العالية الخاصة بالضحية.

ولنتوقف قليلاً عند حالة الدخول بصلاحيات مدير النظام-System Administra) (tor أو (Supervisor) والتي ذكرنا سابقًا أنها كثير ما تكون بغير حدود. وهذه الحالة تشكل أكبر خطر يمكن أن يتعرض له النظام.

تستخدم كثير من النظم الآن واجهة (HTML) يقوم من خلالها مدير النظام بأداء مهامه. وتقوم صفحات (HTML) بتنفيذ برامج من نوع (CGI) أو -Common Gate) (way Interface، وهذه البرامج لابد أن تعمل بصلاحيات عالية (Root privileges). فإذا تمكن أحد المستفيدين في الشبكة الداخلية من إرسال حزم (HTTP) إلى خادم النسيج لتعمل بهذه الصلاحيات، فمن السهل على هذا المستخدم أن يخدع خادم النسيج ليجعله يقوم بتنفيذ ما يشاء من برامج. ويستطيع هذا المستفيد أن يفعل ذلك عن طريق الدخول أولاً باستخدام رمز المستفيد (UID) وكلمة السر الصحيحة، والمعتاد عند إتمام التحقق من شخصية هذا المستفيد ألا يتم إجراء المزيد من التحقق بعد ذلك، ومن ثم يستطيع المهاجم انتحال عنوان جهاز الحاسب الخاص بمدير الشبكة ويرسل ما يشاء من أوامر (HTTP) إلى خادم النسيج ذي الصلاحيات العالية، ومن حسن الحظ أن هذا الهجوم لا يمكن أن يتم من الخارج لأن معظم الشبكات (التي يديرها مسئول أمن مدرب) لا تسمح بالدخول عن بعد إلى خادم نسيج ذي صلاحيات عالية (Root)، ولكن بعض الجهات تستخدم جهازًا واحدًا كخادم نسيج وفي نفس الوقت يستخدم الجهاز كخادم قاعدة بيانات (أي يحتاج الجميع إلى استخدامه!) ولذلك ننصح باستخدام طبقة المدخل الآمنة (SSL) أو (Secure Socket Layer) والتي تعتمد على تقنيات التشفير باستخدام المفتاح العلني (Public key)، أو استخدام مواصفة

(IPsec) القياسية التي تضمن أمن حزم رسائل الإنترنت في الشبكة، وتصميم هذه المواصفة مرن بما فيه الكفاية لدعم مجموعة من خوارزميات التشفير. وتعمل مواصفة (IPsec) عن طريق ضمان " الربط الآمن " (Security association) بين نقطتين، والذي يحتوي على العديد من المعاملات حول أسلوب تبادل المعلومات بين هاتين النقطتين بما في ذلك أسلوب التشفير المستخدم. فيستخدم " مقدمة التحقق من الشخصية " (AH) أو (Authentication Header)التي تضمن التحقق من الشخصية.

٨-٣ إجراءات تطبيق نظم كشف الاقتحام:

ذكرنا من قبل أن نظم كشف الاقتحام (IDs) الموجودة في الأسواق حاليًا لا يمكن أن تعمل وتنجح في كشف عمليات الاقتحام بمفردها، وإنما من الضروري أن تعمل مع باقي أدوات أمن المعلومات في منظومة أمنية متكاملة بحيث تتبادل هذه الأدوات المعلومات وتوزع الأدوار فيما بينها، وقدمنا في الفصل السابق (٧-٢) عرضًا للأجهزة الحديثة لمراقبة الشبكات.

تعتمد الكثير من نظم كشف الاقتحام في أداء مهمتها على تحليل ما يقوم بتسجيله نظام التشغيل (OS audit trail)، ومن ثم تشكل هذه المعلومات "البصمة" التي تكشف كيف كان أداء النظام عبر فترة معينة من الزمن. وهذه المعلومات متاحة ويسهل الحصول عليها في جميع النظم وتشكل أساسًا ممتازًا يمكن من خلاله تحليل أداء النظام، لحظة بلحظة، ومن ثم معرفة إذا كان النظام يتعرض الآن للانتهاك (الاقتحام) أم لا.

ولا تكتفي نظم كشف الاقتحام بهذه المعلومات وإنما تقوم بجمع المعلومات الخاصة بها عن طريق مراقبة النظام الذي تجري حمايته، وذلك باستخراج إحصاءات معينة من مجموعة من المصادر المتاحة مثل: معدل استخدام وحدة المعالجة المركزية (CPU usage)، عمليات الإدخال والإخراج على القرص (Disk I/O)، استخدام ذاكرة النظام خلال هذه الفترة،

الأنشطة التي قام بها المستخدمون وعدد محاولات الدخول إلى النظام، ... إلى آخره. ومن البديهي أن هذه الإحصاءات يجب أن يتم تحديثها أولاً بأول لكي تعكس الوضع الراهن للنظام. وتتم مراجعة هذه الإحصاءات في ضوء نموذج داخلي مخزن في قاعدة بيانات نظام كشف الاقتحام حتى يسمح لنظام كشف الاقتحام بتحديد ما إذا كانت هذه السلسلة من العمليات التي رصدها، تشكل احتمال حدوث اقتحام للنظام الذي تجري مراقبته. هذا النموذج في العادة يصف مجموعة من " السيناريوهات " لعمليات الاقتحام، أو قد يصف، على العكس من ذلك، خصائص النظام السليم الذي لا يحدث له اقتحام. وعن طريق مقارنة هذا النموذج بما يتم جمعه من معلومات عما يجري يستطيع نظام كشف الاقتحام تحديد إذا ما كان هناك اقتحام يجري أم لا.

٨-٢-١ مواصفات نظام كشف الاقتحام:

الآن ما هي مواصفات نظام كشف الاقتحام الجيد؟ وما هي الاعتبارات التي يجب أن نهتم بها عند اختيارنا لهذا النظام؟

يجب أن تتوفر في نظام كشف الاقتحام الجيد مجموعة من الخصائص [Kaeo ١٩٩٩]:

(١) يجب أن يعمل " طوال الوقت " دون أي توقف ودون الحاجة إلى أي إشراف بشري. ويجب أن يكون النظام موثوقًا به بدرجة كافية لكي يمكن السماح له بالعمل باستمرار في خلفية النظام الذي تجري مراقبته. ومن المهم أن نعرف أن نظام كشف الاقتحام لا يجب أن يكون " صندوقًا أسود " غير معلوم ما بداخله. بل يجب أن تكون محتوياته معروفة وأسلوب عمله قابلاً للفحص من الخارج.

(٢) يجب أن يكون قابلاً لتصحيح الأخطاء التي قد تقع (Fault tolerant)، أي أنه يجب أن ينجو في حالة انهيار النظام ويحتفظ بما في " قاعدة المعرفة " (Knowledge-base) الخاصة به من بيانات، لا أن يتم حذف المعلومات التي تحتويها هذه القاعدة عند إعادة تشغيله.

(٣) يجب أن يكون النظام قادرًا على مقاومة محاولات تعديله أثناء عمله (Subversion)، فيجب أن يقوم بمراقبة أدائه بنفسه للتأكد من أن أحدًا لا يحاول تعديله، كما يجب أن يقاوم محاولة أن يقوم شخص ما بتغييره ويضع مكانه نظامًا آخر.

(٤) يجب ألا يشكل عبئًا (overhead) على النظام الذي تتم مراقبته، فالنظام الذي يبطئ من أداء الحاسب الذي يراقبه إلى درجة غير مقبولة لن يكون قادرًا على العمل أو الحماية، فضلاً عن منع النظام نفسه من العمل.

(٥) يجب أن يكون قادرًا على ملاحظة أي انحراف للنظام الذي يقوم بمراقبته عن الأداء الطبيعي المعتاد.

(٦) أن يمكن دمجه بسهولة مع النظام الذي تجري مراقبته، فكل نظام من النظم التي تتم مراقبتها يكون له نمط استخدام مختلف ، وبالتالي فإن الآلية الدفاعية يجب أن تتواءم بسهولة مع هذه الأنماط ولا تتعارض معها ولا يكون أداؤها متعارضًا مع ما يقوم به النظام الذي تتم مراقبته.

(٧) يجب أن يكون قادرًا على التوافق مع التغييرات التي قد تطرأ فيما بعد على النظام الذي تتم مراقبته، مثل أن يتم استحداث تطبيقات جديدة، فأي نظام يمكن أن تتغير طبيعته ومكوناته بمرور الوقت، ونظام كشف الاقتحام يجب أن يكون قادرًا على التوافق مع هذه التغيرات.

(٨) في النهاية يجب أن يكون نظام كشف الاقتحام غير قابل للخداع، أي أن يكون من الصعب على المقتحم تضليله بأي شكل، وأن يكون كذلك غير قابل للتجاوز أو تحييد عمله من جانب المقتحمين.

٨-٣-٢ أساليب خداع نظم كشف الاقتحام:

يمكن لبعض المقتحمين (Hackers) خداع نظم كشف الاقتحام عن طريق عدة سبل يمكن حصرها في: " الإنذار الكاذب بالاقتحام " (False positive)، و" عدم الإنذار في

حـالـة الاقـتحـام "(False negative)، و" إقحـام نسخـة أخـرى من البـرنـامج " (Subversion) [Purdue ٢٠٠٣].

فيحدث " الإنذار الكاذب بالاقتحام " عندما يفسر نظام كشف الاقتحام بعض الأفعال أو الرسائل بأنها عملية اقتحام بينما هي في الحقيقة عملية مشروعة، بينما يحدث " عدم الإنذار في حالة الاقتحام " عندما يقع اقتحام حقيقي ولكن نظام كشف الاقتحام يسمح بمروره باعتباره عملاً مشروعًا، أما " إقحام نسخة أخرى من النظام " فيحدث عندما يقوم المقتحم بتعديل عمل نظام كشف الاقتحام بهدف دفعه إلى " عدم الإنذار في حالة الاقتحام ". دعنا نلقي نظرة أكثر قربًا على كل من هذه الأساليب الثلاثة لخداع نظم اكتشاف الاقتحام.

٨-٣-٢-١ الإنذار الكاذب بالاقتحام (False Positive):

في كثير من الأحيان يأتي " الإنذار الكاذب بالاقتحام" (False positive) عفويًا وبشكل غير متعمد نتيجة تفسير خاطئ لبعض العمليات التي تحدث. ويدفع الإنذار الكاذب مستخدمي نظام كشف الاقتحام على المدى الطويل إلى تجاهل إنذاراته وعدم فحص مخرجاته لأنه يصنف الأعمال المشروعة باعتبارها اقتحامًا، وينتهي الأمر بتجاهل كل الإنذارات فيفقد النظام الهدف منه. ولذلك يجب تجنب حدوث هذا الأمر بقدر الإمكان (إذ إنه من المستحيل إلغاؤه تمامًا).

٨-٣-٢-٢ عدم الإنذار في حالة الاقتحام (False Negative):

أما " عدم الإنذار في حالـة الاقتحـام " (False negative) فهو يسمح بمرور التصرفات العدائية. وهو أمر أكثر خطورة من سابقه لأنه يعطي إحساسًا زائفًا بالأمن. وبتمرير كل العمليات فلن تلفت العمليات المشبوهة نظر مسئول الأمن الذي يجد أن كل شيء على ما يرام، خاصة أن كثيرًا من عمليات الاقتحام تبدأ وتنتهي دون أن تترك

وراءها ضررًا ظاهرًا كزجاج مكسور أو قفل مغتصب أو بصمات على الخزانة، بل قد تبدأ الجريمة وتنتهي (بل وتتكرر) دون أن يلفت ذلك الأنظار، مما يجعلنا نؤكد أن السماح بتكرار هذا الأسلوب من الخداع " عدم الإنذار في حالة الاقتحام " يجعل النظام أقل أمنًا مما كان قبل تركيب نظام كشف الاقتحام!!.

٨-٣-٢-٣ إقحام نسخة أخرى من البرنامج (Subversion):

الأسلوب الثالث من أساليب الخداع وهو " إقحام نسخة أخرى من البرنامج " (Subversion) ربما كان أخطرها وأكثرها تعقيدًا، وهو مرتبط دائمًا بالأسلوب الثاني " عدم الإنذار في حالة الاقتحام ". وفي هذه الحالة يستخدم المقتحم معلوماته عن تفاصيل نظام كشف الاقتحام في تعديل أداء هذا النظام لمهامه بما يدعه يمرر العمليات العدائية دون أن يصدر إنذارًا بها، ومن ثم يستطيع المقتحم انتهاك كافة احتياطات الأمن الموضوعة. هذا الأمر قد يمكن اكتشافه بواسطة مراقب بشري عند قيامه بفحص سجل العمليات (Logs) التي يخرجها نظام كشف الاقتحام، ولكن للأسف سيظل ما يبدو على السطح هو أن النظام يعمل وأن الأمور كلها على ما يرام.

من بين الصور التي يحدث من خلالها الأسلوب الثالث هي خداع نظام كشف الاقتحام بالتدريج وعبر الزمن، فقد يواجه النظام بمجموعات من العمليات إذا أخذت كل منها على حدة فإنها تبدو بريئة ولا تشكل تهديدًا للنظام، ولكن عند تكرار هذه العمليات فإنها تسبب انهيار النظام أو توقفه. كيف يكون ذلك؟ ذكرنا سابقًا أن نظام كشف الاقتحام يقوم باستمرار بتحديث معلوماته ويضع لنفسه نموذجًا للأداء السليم للنظام، ومن ثم يستطيع اتخاذ القرار بشأن أي عملية بمقارنتها بهذا النموذج. فإذا استطاع المقتحم خلال فترة من الزمن تمرير بعض العمليات التي تختلف شيئًا فشيئًا عن النموذج الذي يحتفظ به النظام، فمن الممكن في النهاية أن يتم قبول هذه العمليات باعتبارها عمليات مشروعة، بينما هي في الحقيقة جزءًا من عملية اقتحام ذكية (شيء يشبه القتل البطيء بدس السم تدريجيًا مثلما تعرض له نابليون بونابرت على يد

الإنجليز في منفاه بجزيرة سانت هيلانة).

٨-٣-٣ مواصفات الأجهزة المستخدمة في النظام:

ذكرنا في بداية هذا الفصل أن نظام كشف الاقتحام يتكون من جزأين:

- الآلة " (Engine)التي تقوم بفحص الرسائل المارة.
- و" أداة المراقبة " (Console)التي يتم من خلالها إدارة " الآلة " وإخراج التقارير المطلوبة.

هناك بعض النظم المعروضة في الأسواق التي تدمج الاثنين في جهاز واحد يقوم بالمهمتين معًا، أي الفحص والإدارة. ولكننا لا ننصح بذلك بل نفضل أن يكون الجهازان منفصلين وذلك تحسبًا لتركيب عدة " آلات " (Engines) أخرى في المستقبل وأن تتم إدارتها جميعًا من جانب أداة المراقبة (Console).

ويجب أن يكون للآلة (Engine) مواصفات عالية إذ إن معظم الرسائل تمر بها ولذلك يجب ألا تكون عائقًا في سبيل حسن أداء الشبكة، فلا يجب أن تقل الذاكرة الرئيسية عن (٥١٢ MB) وألا تقل سرعة المعالج عن (١ Ghz) ، وطالما أن النظام سيستخدم قاعدة بيانات وملف لتسجيل الوقائع (Log) فيجب ألا تقل مساحة القرص الصلب المتاحة عن (٤٠ GB) إلا إذا كان معدل مرور الرسائل عبر الشبكة محدودًا جدًا. وربما زادت احتياجات القرص الصلب في جهاز المراقبة الذي يتعامل مع عدة آلات (Engines)، حيث يتطلب الأمر احتفاظ أداة المراقبة (Console) بنسخة من قواعد البيانات الموجودة في الآلات جميعها للاستفادة منها في إصدار التقارير، فنحتاج إلى طاقة تخزين إجمالية لا تقل عن (١٠٠ GB).

٨-٤ بعض نظم كشف الاقتحام الحديثة وتقييمها:

نقدم فيما يلي عرضًا لبعض نظم كشف الاقتحام الحديثة والأكثر انتشارًا في

الأسواق في الوقت الحالي وتقييمها.

٨-٤-١ نظام (eNTrax):

هذا النظام تملكه شركة " سيبرسيف " (Cybersafe Corporation) وهو عبارة عن مجموعة نظم تهدف لكشف عمليات الاقتحام، وهو يقوم بهذه المهمة مستخدمًا نظام تشفير مدعم من شركة " سيبرسيف ". وأسلوب عمل هذا النظام هو تسجيل الوقائع باستمرار، ويقوم جهاز مراقبة التحليل على فترات زمنية محددة بإرسال بيانات الوقائع المسجلة (Log) ليتم فحصها، كما أن النظام يمكنه فحص البيانات بمجرد تسجيلها (Real time) بدلاً من الانتظار حتى انقضاء الفترة المحددة. ومن خلال الوقائع المسجلة يتم إجراء تحاليل لاستنتاج الاتجاهات المستقبلية باستخدام أدوات " تعدين البيانات " (Data mining) التي يتضمنها النظام. وهكذا يقوم النظام بمهمة كشف الاقتحام على مستوى الحاسب المضيف (Host-based) مما يمنح محلل عمليات الاقتحام القدرة على تحديد الأنشطة العدائية التي قد يقوم بها مستخدم ذو صلاحية، أو مستخدم حصل على صلاحية بطريقة غير مشروعة.

كما يقوم النظام بكشف الاقتحام على مستوى الشبكة (Network-based) بواسطة مجس يفحص الرسائل الواردة من خلال بروتوكول (TCP/IP) لتحديد ما يهدد الشبكة، وهو ما يمنح محلل عمليات الاقتحام نفس القدرات التي تمنحها نظم (Host-based) في الأحوال التي تستخدم فيها الشبكة للحصول على المعلومات المحظورة.

ثالث مجالات العمل التي يقوم بها هذا النظام هو تقييم درجة ضعف النظام (Vulnerability assessment) وهي من أبرز مزاياه. ويقوم النظام، لأداء هذه المهمة، بتشغيل أحد البرامج على أجهزة الحاسب الرئيسية في الشبكة، ويجري هذا البرنامج عددًا من اختبارات التهيئة (الداخلية) ويرسلها إلى أداة المراقبة (Console)، وتقوم النسخة الحديثة من هذا البرنامج بأداء هذه المهمة (خارجيًا) أيضًا بمعنى فحص الشبكة نفسها وليس الأجهزة المستضيفة فقط.

المهمة الرابعة للنظام هي تنفيذ السياسات الرقابية؛ فالسياسة الرقابية هي الأسلوب المتبع لتوجيه النظام للتركيز على بعض الأحداث المهمة دون غيرها. ولتوضيح ذلك نذكر مثلاً أن جمع العديد من البيانات يؤثر على أداء النظام مما يعطل وسائل جمع البيانات نفسها! ومن ناحية أخرى فإن تجاهل العديد من الرسائل سوف يعطي إحساسًا زائفًا بالأمان (False negative) ولذلك فإن توجيه النظام ضروري للوصول إلى منطقة وسط.

هذا النظام يعتبر نظامًا جيدًا إذا كنا نستخدم في المؤسسة نظام التشغيل (Windows NT)، وإذا كانت المعلومات المخزنة في قواعد بيانات المؤسسة على جانب كبير من الأهمية.

٨-٤-٢ نظام (CMDS):

هذا النظام " نظام كشف سوء استخدام الحاسب" (CMDS) أو (Computer Misuse Detection System) من شركة (ODS Network) هو نظام لكشف الاقتحام وسوء الاستخدام معًا، وهو مصمم للمؤسسات الكبيرة. يستخدم هذا النظام نظام " خادم/عميل " مع أكثر من خادم قاعدة بيانات مركزي لإتاحة تصور شامل للحالة الأمنية للشركة أو المؤسسة بالكامل. ويستطيع نظام (CMDS) تحليل البيانات الواردة من المقر الرئيسي للشركة ومن فروع الشركة أو المؤسسة وربط كافة الوقائع معًا لاكتشاف احتمالات سوء الاستخدام.

ونظام (CMDS) شأنه شأن نظام (eNTrax) يقدم أدوات عديدة تسهل جمع وتحليل وقائع الاستخدام، والبيانات المختلفة التي يولدها النظام نفسه. وهذه البيانات يتم ضغطها وتشفيرها قبل تخزينها، وعند الفحص تتم إعادتها إلى حالتها الأصلية.

ويعمل مسئول الأمن على أداة المراقبة (Console) من خلال واجهة مستفيد جيدة يستطيع من خلالها الحصول على التقارير المطلوبة والرسوم البيانية الناتجة عن تحليل

البيانات. كما يضم النظام نظامًا خبيرًا (Expert system) إلى جانب حزمة برامج إحصائية. ويتم جمع المعلومات من مصادر عدة، مثل الموجهات وجدران الحماية للحصول على صورة كاملة عما يحدث، ولعل هذه النقطة بالذات (جمع كل ما يمكن من معلومات) هي من أهم ما يميز نظام كشف اقتحام عن الآخر.

ويقوم النظام الخبير الذي يشكل جزءًا من هذا النظام بتقييم كل الوقائع المسجلة ومقارنتها بالمعلومات التي لديه والتي يمكنها تمييز الوقائع البريئة من الوقائع المشبوهة. ويستطيع مستخدم النظام إثراء النظام الخبير بالمزيد من النماذج المشبوهة. وتقوم البرامج الإحصائية بمقارنة العمليات الجارية بما هو مخزن لديها لاكتشاف أي خروج عن المألوف مما يشك أن يكون سرقة للمعلومات أو لرموز المستفيدين أو كلمات السر الخاصة بهم.

تنقسم مهمة أداة المراقبة (Console) إلى جزأين شأنها شأن أي نظام كشف اقتحام وهما: تحذير مسئول الأمن من العمليات المشبوهة، والثانية تقديم أداة للتقييم الفوري لحجم المشكلة، ويستطيع مسئول الأمن في نظام (CMDS) عبر هذه الأداة مراجعة واقعة معينة وكل ما يتعلق بها من بيانات ويستعرضها على شاشة أداة المراقبة.

وفي النهاية .. علينا أن نعلم أن هذا النظام يصلح للمؤسسات الكبيرة ذات الفروع المتعددة والتي لديها كم كبير من المعلومات الحساسة، ولكنه يتطلب تكلفة عالية سواء لاقتنائه أو تشغيله وصيانته وتحليل ما يخرجه من معلومات.

٨ـ٤ـ٣ نظام (Tripwire):

نظام (Tripwire) لكشف الاقتحام هو واحد من أوائل نظم كشف الاقتحام التي تم تطويرها في جامعة " بوردو " بواسطة كل من " جيم كين " و" جين سبافورد " [Northcutt ١٩٩٩] وله موقع يمكن الحصول عليه منه وهو موقع " تريب واير "

[tripwire ٢٠٠٣]. وترتكز فكرة النظام على حقيقة مفادها أن أي اقتحام لابد أن يتبعه تعديل ما في أحد الملفات. ولذلك يركز النظام على اختبار سلامة الملفات، فيمر على ملفات النظام ويقوم بتوليد رقم شفري لكل ملف. لذلك يفضل تشغيل نظام (tripwire) على جميع ملفات النظام والحصول على نسخة احتياطية من قاعدة البيانات التي يخرجها النظام على قرص وحفظها في مكان أمين مع ترك الأصل على الخادم. ويقوم النظام دوريًا (يحدد مسئول أمن النظام معدل التنفيذ) بالمرور على الملفات وإعادة توليد الأرقام الشفرية ومقارنتها بالأصل. وعادة يقوم مسئولو أمن المعلومات بتعديل قائمة الملفات المحفوظة لتقليل حالات " الإنذار الكاذب بالاقتحام " إلى أقصى حد ممكن وتفادي احتمالات " عدم الإنذار في حالة الاقتحام ".

برغم أن هذا النظام محدود الانتشار إلا أن له ميزة هامة وهي أن يؤكد لمسئول أمن المعلومات عدم حدوث اقتحام لم يعلم به في حينه. فلا توجد وسيلة في العالم على وجه الإطلاق تؤكد لك أن نظامك لم يحدث عليه اختراق! نعم هذا حقيقي، ولكن هذا النظام (tripwire) إذا اكتشف عدم حدوث أي تعديل في ملفات النظام فإنه يعتبر ذلك نوعًا من التأكيد على عدم حدوث اختراق في الفترة التي انقضت منذ آخر (بصمة) تم أخذها لملفات النظام (تلك البصمة التي تم حفظها في مكان أمين، فالبصمة الموجودة على الجهاز لا يمكن الاطمئنان إلى سلامتها فهي عرضة للاختراق).

ولابد أن نوضح أن هذا النظام (إذا حسبناه ضمن نظم كشف الاقتحام) يعاني من زيادة حالات " الإنذارات الكاذبة بالاقتحام " نظرًا لتغير العديد من الملفات خلال الفترات الواقعة بين كل مرة يتم فيها تشغيل النظام. ولتفادي ذلك فإن بعض الملفات التي يكثر تعديلها يتم حذفها من قاعدة بيانات النظام، ولكن ذلك بالطبع سيؤدي إلى زيادة حالات " عدم الإنذار في حالة الاقتحام ".

وهناك أنواع أخرى من هذه النظم التي تعني بسلامة الملفات مثل (L٥) و(SPI) [Northcutt ١٩٩٩].

٨-٤-٤ نظام (nmap):

هذا النظام (nmap) هو في الحقيقة أداة لتقييم درجة ضعف النظام (Vulnerability assessment)، أو " ماسح للنظام "(Scanner)، ولقد أوردناه هنا حتى نغطي كافة أنواع نظم كشف الاقتحام. وهو يعتبر من أفضل النظم المستخدمة مع نظام التشغيل " يونكس " (UNIX) وأكثرها انتشارًا، وصدرت منه مؤخرًا نسخة يمكنها العمل مع نظام التشغيل (Windows NT).

ويقوم النظام بجمع العديد من المعلومات المتاحة، ولذلك يستخدمه المقتحم كما يستخدمه المدافع نظرًا لأهمية المعلومات التي يجمعها ونظرًا لقدرته على تقييم درجة ضعف النظام واكتشاف نقاط الضعف فيه. ويتم تحسين النظام باستمرار من جانب مطوريه ومن جانب الكثير من الجهود التطوعية التي تضيف إلى النظام حتى كاد أن يكون أحد النظم المفتوحة التي بدأت تنتشر الدعوة إليها هذه الأيام. يقوم النظام بجمع المعلومات عن النظم المهاجمة وذلك عن طريق إرسال حزمة (TCP) غير صحيحة (invalid) إلى النظام الذي يشك في أنه يحاول الاقتحام، وهذه الحزم غير الصحيحة يعالجها كل نظام تشغيل بشكل مختلف. وبناء على رد نظام التشغيل المعادي يستطيع نظام (nmap) التعرف على نوع نظام التشغيل عن طريق مقارنة رده على الحزم غير الصحيحة مع الردود الموجودة في قاعدة البيانات المخزنة لديه ثم " يستنتج " نوع نظام التشغيل ونسخته.

نفس هذا السلاح يستخدمه المقتحمون الذين يودون معرفة نوع نظام التشغيل الذي يعمل على خادم الشبكة التي تتم مهاجمتها وبذلك يعطيهم أداة لا تقدر بثمن. وعن طريق تحليل البصمات التي يتركها المهاجم وتصنيفها إلى أنماط فرعية (Subpatterns) نستطيع التمييز بين البصمة الناتجة عن محاولة اقتحام ناجحة وتلك الناتجة عن محاولة اقتحام فاشلة. ولذلك فإن النظام يستفيد كثيرًا من المحاولات التي يقوم بها مقتحم ذكي! فنظام (nmap) يثري قاعدة بياناته بالبصمات الناتجة عن هذه الأنواع الذكية من الهجوم (نوع من النظم الذكية التي تتعلم عبر تشغيلها). هذه

الأنواع من الهجوم من المحتمل جداً أنها كانت ستمر بنجاح في المؤسسات التي لا تقتني هذا النظام أو أنظمة مشابهة.

٨-٥ تحليل عمليات الاقتحام بعد حدوثها:

عادة يكون تحليل عمليات الاقتحام عن طريق فحص وقائع الاستخدام وعمليات التعديل والحذف التي تجري على البيانات، ومتابعة شكوى المستخدمين من سوء أداء النظام، والأنماط المعتادة للرسائل الواردة، ومعدلات الاستخدام في الأوقات المختلفة، ومحاولات الدخول الفاشلة وغير ذلك. ولكي يمكن اكتشاف أي تصرفات مشبوهة تخالف أنماط العمل العادية يجب أن نحتفظ بسجلات تاريخية لأنماط العمل العادية (المقبولة) سواء من ناحية مستوى الأداء أو معدلات الاستخدام أو أنماط الرسائل. لذلك تعتمد معظم نظم كشف الاقتحام على مزيج من " نظم التحليل الإحصائي " و" نظم تحليل القواعد المسجلة ". أما بالنسبة لنظم التحليل الإحصائي فهي تحتفظ بسجلات تاريخية لكل مستخدم ولكل نظام تتم مراقبته، وتصدر نظم " التحليل الإحصائي " إنذاراً عندما يبدأ النشاط الذي يتم فحصه في الانحراف عن أنماط الاستخدام المتوقعة والمقبولة. ويهدف هذا النوع من التحليل إلى كشف المقتحمين الذين يتخفون في صورة مستخدمين شرعيين. كما يستطيع التحليل الإحصائي كذلك كشف المقتحمين الذين يستفيدون من الثغرات الأمنية التي لا يعلم بها مسئولو أمن النظام، وعادة تكون هذه هي الطريقة الوحيدة التي تمكن من كشف هذه الثغرات.

أما نظم " تحليل القواعد المسجلة " فتستخدم عدداً من القواعد التي تصف سيناريوهات الاقتحام المعروفة وتصدر إنذاراً إذا طابق النشاط الذي يتم فحصه أياً من هذه القواعد المسجلة. ويهدف هذا النوع من التحليل لكشف محاولات استغلال الثغرات الأمنية المعروفة في النظام الذي تتم مراقبته. كما يمكن باستخدام هذا النوع من التحليل كشف المقتحمين الذين يظهرون خلال محاولة الاقتحام نمطاً سلوكياً معيناً معروفاً للنظام، أو نمطاً يتعارض مع السياسة الأمنية للموقع. ومعظم النظم التي

تستخدم أسلوب تحليل القواعد المسجلة يمكن تعديلها بواسطة المستفيد عند الحاجة، بينما يمكنه تعريف القواعد الخاصة به. وفي بعض الأحيان يكون الحل الوحيد أمام القائم بالتحليل هو إغلاق النظام أو على الأقل فصله عن الشبكة.

وعند تحليل الوقائع بعد حدوثها يجب اتباع خطوات محددة ويجب أن تكون هذه الخطوات مسجلة بوضوح ضمن السياسة الأمنية للمؤسسة، ويمكن تلخيص هذه الخطوات فيما يلي:

٨-٥-١ ترتيب أولويات الإجراءات:

الخطوة الأولى هي ترتيب أولويات الإجراءات التي سيتم اتخاذها خلال تحليل الواقعة، وتهدف هذه الخطوة إلى تجنب الاضطراب عند حدوث الواقعة وعدم معرفة فريق التحليل من أين يبدأ. ويجب أن تعكس الأولويات السياسة الأمنية للمؤسسة.

٨-٥-٢ تقييم الأضرار الناجمة:

هذه الخطوة ليست خطوة سهلة وهي قد تستغرق وقتًا طويلاً، وتتضمن تحديد أثر الاقتحام وتقييم مدى الضرر الذي أصاب المؤسسة بسببه، وفي هذه الخطوة يتم فحص كافة أجزاء الشبكة، إذ إن كل هذه الأجزاء تصبح موضع شبهة، وذلك بهدف تحديد الأنظمة الفرعية التي تعرضت للاقتحام. فيتم فحص جميع الموجهات (Routers)، والمحولات (Switches)، وخادم الشبكة (Network access server)، وملف تهيئة جدار الحماية، وملفات تهيئة باقي الخوادم التي تقدم الخدمات المعاونة للشبكة الرئيسية مثل خادم البريد الإلكتروني (e-mail server)، وخادم الطباعة(Print server) وغيرها؛ فتهيئة هذه الأجهزة يمكن التلاعب فيها تمهيداً لاقتحام تال.

كما يجب تحليل سجل الوقائع للرسائل المارة بالشبكة (Traffic log) لتحديد أي أنماط غير عادية لهذه الرسائل. كما يجب فحص الشبكة عن طريق برنامج الفحص

المصـاحب لنظـام التشـغيل والذي يكشف عن أي أجهزة جديدة قد تكون أضيفت إلى الشبكة، كما يجب فحص البيانات المهمة والملفات الحساسة للتأكد من عدم خضوعها للتعديل، ويجب الاهتمام بفحص كلمات المرور الخاصة بالنظم الحساسة للتأكد من عدم تعديلها.

٨-٥-٣ إجراءات الإبلاغ والإنذار:

يجب أن يكون لدى المؤسسة أسلوب منهجي للإبلاغ عن هذه الحوادث، ومن ثم إخطار الجهات المعنية، ويجب أن يتم ذلك بأسرع وسيلة ومع توفير كل المعلومات الممكنة. ولذلك يجب أن يكون لدى المؤسسة خط هاتفي (ساخن) يعمل على مدار الساعة لاستقبال مثل هذه البلاغات، كما يجب أن يكون لديها عنوان بريد إلكتروني خاص.

وعلى الفريق الذي سيتعامل مع الواقعة أن يقوم بدوره بإبلاغ كل من يلزم إبلاغهم، إما عن طريق الهاتف أو باستخدام القوائم البريدية الإلكترونية (e-mail lists) ويجب أن يتم مسبقًا تحديد من تضمهم هذه القوائم وتصنيفهم، كأن تكون هناك قائمة للمديرين، وأخرى للمستفيدين، وأخرى لمسئولي الشبكة وهكذا. كما يجب إخطار مقدم الخدمة (Service provider) والمواقع الأخرى المتصلة بالشبكة خاصة إذا كان الموقع جزءًا من شبكة خاصة افتراضية (VPN)، ويجب الاهتمام بالنقاط التالية عند حدوث مثل هذه الحوادث:

- عدم إفشاء التفاصيل الفنية لواقعة الاقتحام حتى لا يستفيد منها مقتحمون آخرون لاقتحام مواقع أخرى، أو لتفادي اكتشافهم في المرات التالية.
- التعاون مع مسئولي الشرطة لتفادي تدمير الأدلة الجنائية وذلك إذا كان الأمر يستدعي تدخلهم.
- عدم إخفاء الواقعة أو التكتم عليها بدعوى عدم تعريض سمعة الشركة أو البنك للخطر، فهذا التكتم هو أفضل مناخ يعمل فيه المقتحمون.

٨ـ٦ سيناريوهات فعلية لعمليات اقتحام وتحليلها:

نقدم فيما يلي بعض الأمثلة (السيناريوهات) لعمليات اقتحام حدثت في الحقيقة وتحليل هذه العمليات.

٨ـ٦ـ١ السيناريو الأول:

في أكثر من مرة، وفي أوقات مختلفة، حدث انقطاع مفاجئ لاتصال شبكة إحدى الشركات بالإنترنت، ولم يمكن في كل من هذه المرات معرفة السبب. وبمراجعة الرسوم البيانية المستخرجة من تحليل سجلات وقائع الاستخدام للرسائل المارة عبر الشبكة الرئيسية تبين وجود تباين كبير بين عدد الرسائل الواردة وعدد الرسائل المرسلة. فقد تبين أن عددًا كبيرًا من حزم الرسائل التي كانت موجهة إلى شبكة الإنترنت لم يتم الرد عليها، مما كان يشي بأن هناك عملية توليد لعدد كبير من حزم الرسائل من داخل الشبكة إلى خارجها. وتم عندئذ الاستعانة ببعض أدوات التحليل والمراقبة لاختبار البيانات، فتم اكتشاف أن هناك ثلاثة ملايين حزمة رسائل كان يتم توليدها في كل دقيقة من أحد أجهزة الحاسب داخل الشبكة، وأن هذه الرسائل كانت موجهة إلى أحد مواقع المحادثة (IRC) أو (Internet Relay Chating) في روسيا. وقام المسئولون عن أمن الموقع بحجب موقع المحادثة المذكور ظنًا منهم أن هذا سوف يحل المشكلة. وبعد ذلك وخلال الليل حدثت نفس الواقعة مرة أخرى ولكن مع موقع آخر في هولندا مما تسبب مرة ثانية في انقطاع الاتصال بشبكة الإنترنت. في هذه المرة كان مسئولو الأمن أكثر انتباهًا وتم تحديد الجهاز المستخدم والشخص الذي يستخدمه من داخل الشركة. وتبين أن هذا الشخص كان يستخدم الجهاز بهدف مهاجمة هذا الموقع (موقع المحادثة)، فقد كان يقوم بتشغيل نسخة من برنامج (Spray) الذي يقوم بإغراق الجهة المرسل إليها بفيض من الرسائل. وتبين خلال التحقيق أن الحاسب الفرعي الذي حدث منه الاقتحام به ملف يحتوي على أكثر من ٢٠٠ من رموز المستفيدين تم اختراقها واستخدمت جميعًا في عمليات الهجوم، وبالتالي كان من الصعب التعرف على المقتحم الحقيقي لإغلاق حسابه، وكان هذا الحاسب الفرعي مستخدمًا من جانب آلاف

المستفيدين ولا يمكن فصله عن الشبكة لأهميته للشركة. الحل في هذا الموقف لن يخرج عن أحد إجرائين هما:

(١) إغلاق الحاسب الفرعي وإخطار كافة المستفيدين المتصلين به وتغيير جميع كلمات السر المستخدمة.

(٢) فصل الحاسب الفرعي عن شبكة الإنترنت وحرمان كافة المستخدمين من استخدام الإنترنت.

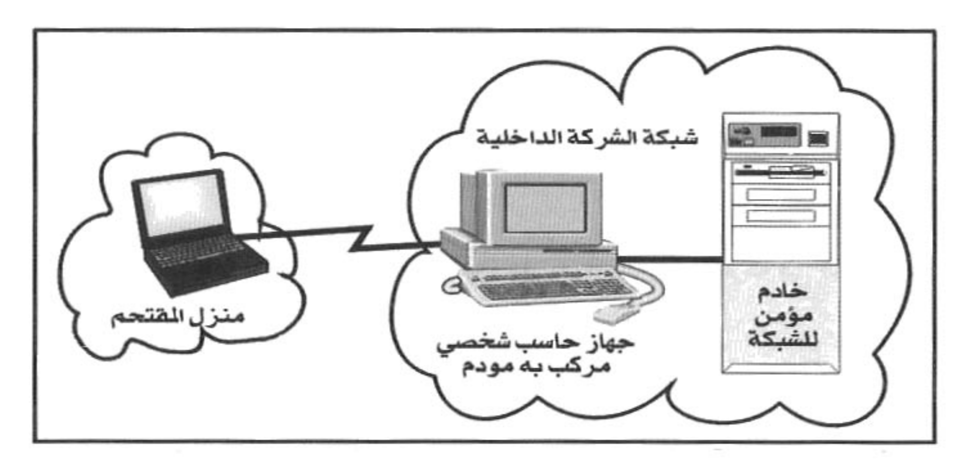
واختيار أحد الحلين يتوقف بدرجة كبيرة على قرار إدارة الشركة في التصرف في مواجهة هذا السيناريو والاحتمالات التي ستترتب على القرار.

٨-٦-٢ السيناريو الثاني:

ربما كان الاقتحام بواسطة شخص من الداخل لجهات خارج الشبكة أقل خطورة ولكن في السيناريو التالي كان الأمر جاداً وخطيراً.

لوحظ أن هناك محاولات صادرة عن عنوان غير مألوف تحاول الاتصال ببعض الأجهزة في الشبكة الداخلية والتي تحتوي على بيانات حساسة، وبدلاً من فصل الشبكة عن الإنترنت ومنع ألف مستخدم من الاتصال بها فقد قرر مسئول الأمن استمرار الاتصال لبعض الوقت وتتبع مصدر هذه المحاولات، و لكنه لم يستطع التعرف على هذا المصدر، وسرعان ما تبين، بمزيد من البحث، أن المقتحم هو أحد العاملين بالشركة، ولكنه قام بالاتصال من منزله بالهاتف الداخلي في مكتبه بالشركة الذي كان متصلاً بالحاسب الشخصي المخصص له عن طريق " مودم ". وكان هذا الشخص قد قام بتركيب المودم في الحاسب الشخصي الموجود بمكتبه في وقت سابق. وبمجرد تمكنه من الدخول إلى حاسبه الشخصي في الشركة فقد أمكنه الدخول إلى باقي الشبكة كما يبين الشكل (٨-١).

شكل (٨-١)
اقتحام شبكة الشركة عن طريق الاتصال بمودم مركب في أحد الأجهزة



٨ـ٧ أجهزة كشف الاقتحام:

توجد الآن في الأسواق أجهزة (Hardware) تقوم بمهمة كشف الاقتحام. وهذه الأجهزة تنافس بشدة استخدام البرمجيات من خلال حاسبات شخصية عادية، وسبب المنافسة الشديدة هو أن نظم كشف الاقتحام التي تحمي الشبكات تواجه ثلاثة تحديات مهمة وهي:

١- تشفير حزم البيانات، فكيف يمكننا التأكد من أن محتوى الرسالة مشفر دون الاختبار العشوائي الذي يستهلك وقتًا كبيرًا من المعالج (CPU) مما يؤثر على الأداء، ومن ثم تظهر ضرورة تنفيذ هذا الاختبار بواسطة الأجهزة (Hardware) لأنها أكثر سرعة بشكل ملحوظ.

٢- الشبكات الجديدة التي تفوق سرعتها سرعة نظم كشف الاقتحام، وهنا يشكل نظام كشف الاقتحام عقبة لا حل لها إلا بالاستغناء عنه!

٣- الشبكات التي تستخدم نظم كشف الاقتحام في المحولات والتي سنتحدث عنها في القسم (٨ ـ ٧ ـ ٢).

وهناك عدة حلول لهذه المشكلات تعتمد كلها على استخدام الأجهزة (Hardware) في تنفيذ كشف الاقتحام.

٨-٧-١ أجهزة (Toasters):

جهاز (Toaster) هو ببساطة جهاز حاسب مصمم للعمل بسرعة تفوق سرعة جهاز الحاسب الشخصي العادي، وهو يمكن أن يكون جهاز حاسب رخيص الثمن يستخدم نظام تشغيل " يونكس " (UNIX) والعديد من التطبيقات الأمنية، فيمتزج هنا الجهاز (Hardware) بالبرمجيات (Software) فيما اصطلح على تسميته (Firmware).

٨-٧-٢ كشف الاقتحام بواسطة المحول:

أفضل مكان يمكن أن تضع فيه أداة كشف الاقتحام هو أن تكون في بطاقة توضع في الموجه (Router) أو المحول (Switch) باعتباره يقع على حدود الشبكة وفي مداخلها. وهو في هذه الحالة يؤدي تمامًا مهمة جهاز (Toaster) [Northcutt ١٩٩٩]. و تجري البحوث حاليًا لتنفيذ (بعض) برامج كشف الاقتحام على الموجه أو المحول مباشرة، وفائدة هذا الاتجاه هو أننا سنحصل على كشف (فوري) للاقتحام؛ ففي جميع الحلول الأخرى (باستثناء تنفيذ برامج كشف الاقتحام على جدار الحماية) لا يتم كشف الاقتحام إلا بعد مرور الحزمة بالفعل، أما في حالة تنفيذ عملية كشف الاقتحام من خلال الموجه أو المحول و(اقتناص) الحزمة قبل مرورها، فإن ذلك يعد خطوة ممتازة في عمليات كشف الاقتحام. ولكن يواجه هذا الأسلوب مشكلة في الشبكات التي تتعدد فيها المحولات، هي أنه من المستحيل اختبار ٢٠٠ مصفاة (Filter) بشكل فوري أو مباشر، ومن المستحيل كذلك كشف كافة عمليات الاقتحام بشكل فوري أو مباشر، ولكن بعضها فقط هو الذي سيتم كشفه فوريًا، أما ما يحتاج إلى مزيد من العمليات فيتم اكتشافه لاحقًا.

٨ـ ٧ـ ٣ الدفاع في العمق:

في الحرب وفي كرة القدم لا يكفي خط دفاع واحد وإلا انكشف الجيش أو انكشف الفريق. وجدار الحماية لا يشذ عن ذلك فهو يفيد كمصفاة توقف العديد من محاولات الاقتحام قبل أن تصل إلى شبكة الشركة أو المؤسسة. أما داخل الشبكة فمن الممكن تهيئة الموجه أو المحول بحيث يراقب مظاهر الاقتحام أو التزوير في الرسائل المارة. وعندما يحدث اكتشاف لعملية مشبوهة يستطيع المحول إما أن ينهي الجلسة ويحجب مصدر الهجوم، أو أن يرسل " إنذارًا صامتًا " (Silent alarm) إلى شاشة أداة المراقبة (Console).

يمكن إضافة خط دفاعي آخر عن طريق إضافة أداة كشف اقتحام على كل جهاز حاسب رئيسي في الشبكة بالإضافة إلى أداة كشف الاقتحام التي تحمي الشبكة كلها. وسوف يسمح ذلك بكشف المهاجمين من الداخل الذين يستخدمون رمز استخدام حقيقي للدخول إلى ملفات محظورة.

بعد استعراض تقنيات الحماية في الفصل السابع، تحدثنا في هذا الفصل بشيء من التفصيل عن واحدة من أهم تقنيات الحماية وهي نظم كشف الاقتحام التي تمثل العين الخبيرة المدربة التي تسهر على حماية الشبكة وتنبه إلى أي محاولة لاقتحامها. ونقدم في الفصل القادم تقنية لا تقل عنها أهمية وهي " جدران الحماية ".

الفصل التاسع
جدران الحماية

في الفصل السابع تحدثنا عن تقنيات حماية شبكات المعلومات ثم تناولنا في الفصل الثامن إحدى هذه التقنيات وهي نظم كشف عمليات الاقتحام، وفي هذا الفصل نتعرض لجدران الحماية، ثم نخصص الفصل العاشر للشبكات الخاصة الافتراضية.

هذا الفصل هو من أهم فصول الكتاب ذلك لأنه يتعرض لجدران الحماية، وجدران الحماية هي أهم وسائل حماية الشبكات وتحقيق أمن شبكات المعلومات. ونبدأ هذا الفصل بقسمين نعرف فيهما جدار الحماية، ثم استخدامات جدران الحماية، وما تستطيع أداءه وما لا تستطيع أداءه. في القسم الثالث نصنف جدران الحماية وفقًا لأسلوب الأداء فنتحدث عن مصافي حزم الرسائل (الاستاتيكية والديناميكية)، وعن خادم البروكسي، ثم نتحدث عن استخدام الأجهزة (Hardware) كجدران حماية. ثم خصصنا القسم الرابع لمقارنة أنواع جدران الحماية فتحدثنا عن مزايا وعيوب مصافي حزم الرسائل، ومزايا وعيوب استخدام خادم البروكسي، ومزايا وعيوب استخدام الأجهزة كجدران حماية، ثم نحاول الإجابة عن سؤالين مهمين: الأول عن أي بيئات التشغيل هي الأنسب لجدران الحماية؟ والثاني عن شراء جدار الحماية هل هو أفضل؟ أم بناؤه أفضل؟ ثم نصل إلى القسم الخامس الذي خصصناه لتصميم جدران الحماية والعوامل التي يجب أن تؤخذ في الاعتبار عند تصميمها. ثم نختم الفصل بشرح كيفية تنفيذ وتطبيق جدران الحماية سواء باستخدام جهاز واحد لتأدية هذه المهمة، أو استخدام خادم الشبكة المحجوب، أو الشبكة الفرعية المحجوبة، أو كيف يمكن أن تتعدد الشبكات الفرعية المحجوبة. ثم نقدم نصائح الاستخدام لكل من الجهات التي تود تركيب جدران الحماية، أو لمقدمي الخدمة وما يجب أن يستخدموه من جدران الحماية.

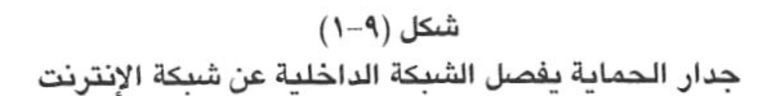
٩ـ١ ما هو جدار الحماية (Firewall)؟

لعله من نافلة القول أن نؤكد أن أي جهة تقدم على الاتصال بشبكة الإنترنت وتقوم بالفعل بتوصيل " خادم الشبكة " (Web server) بالإنترنت دون استخدام " جدار حماية " (Firewall) فإنها تقدم على مخاطرة كبيرة. فإذا تجمع الملايين من البشر في

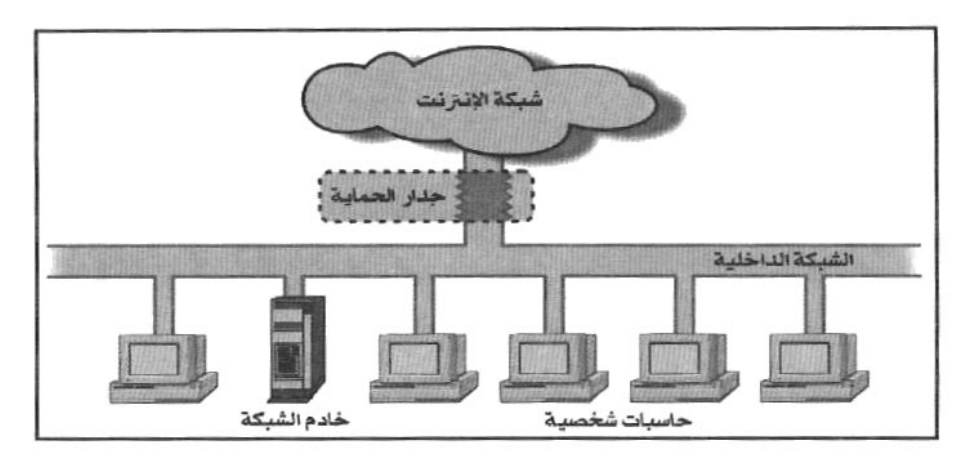
مكان واحد فلابد أن تحدث جريمة، هذا صحيح في المدن وصحيح على شبكة الإنترنت. ومن المخـاطرة كذلك ترك مسـئولية جدار الحمـاية وتهيئته وإدارته لمسئـول الشبكة، فهذا المسئول برغم مـعرفته بالمهمـة التي يقوم بها جـدار الحماية، وبـرغم خبرته بكيفـية تهيئة وإدارة هذا الجهـاز، إلا إنه لا يتنفس أمن المعلـومات، ولا يعـي الأساليب التـي يتبـعها المقتحمـون (Hackers)، ولا يفهم عقليتهم. ومن هنـا نسمـع الكثير عـن شركات (تقتني) جدران حماية ولكنها تعرضت للاختراق أكثر من مرة. ولقد اهتممت بوضـع كلمة تقتني بين قوسين تأكيداً على أن هذه الشركات لا (تستخدم) جدران حماية وإنما تقتنيها فقط، إذ أن المسئول عن إدارتها ليس مسئول أمن المعلومات.

ولعله مـن نافلـة القول أيضـاً أن نـؤكد أن جـدران الحمايـة وحدهـا لا تكفي لحمـاية شبكـة المعلومات وأن منظومة الأمن الشامل تضـم العديد من التقنيـات. ولقد ذكرنا في الفصل السـابق أنه في الحرب وفي كـرة القدم لا يمكن الاعتـماد على خـط دفاع واحد، وإنمـا يجب أن يكون لـدينا أكثر من خط دفاع. وأمـن شبكات المعلـومات لا يختلف في ذلك عن الحرب أو عن كرة القدم.

مهمة جـدار الحماية بصفـة عامة هي منع أخطـار الإنترنت من الوصـول إلى الشبكة الـداخلية للـشركـة أو المؤسـسة، ومـن ثم فمهمـته الأساسيـة هي أن يمنع المهـاجمين من الاقتراب مـن " خطوط الدفاع " الأخرى [Zwicky ٢٠٠٠] ولذلك فـجدار الحماية يوضـع عادة عند نقطة التقاء الشبكة الداخلية بشبكة الإنترنت كما يبين شكل (٩-١).



شكل (٩-١)
جدار الحماية يفصل الشبكة الداخلية عن شبكة الإنترنت



يتبين من الشكل أن كافة الرسائل القادمة من الإنترنت أو المتجهة إليها تمر بجدار الحماية، ومن ثم يكون في مقدور جدار الحماية فحص هذه الرسائل سواء كانت بريداً إلكترونياً، أو ملفات متبادلة، أو محاولات دخول إلى الشبكة عن بعد، أو أي نوع من الاتصال، وبناءً على نتيجة الفحص يقوم بالتصريح لها بالمرور إذا كانت تتفق مع السياسة الأمنية للموقع.

يتكون جدار الحماية في المعتاد من بعض الأجهزة مثل " الموجه "(Router)، وأحد الحاسبات الشخصية، بالإضافة إلى بعض البرمجيات التي تتولى تنفيذ السياسة الأمنية، ولذلك يتم " تهيئة " جدار الحماية لتنفيذ هذه السياسة.

٩-٢ استخدامات جدران الحماية:

سنحاول هنا أن نلخص ما يستطيع جدار الحماية أن يفعله لحماية الشبكة (الداخلية) وما لا يستطيع أن يفعله.

٩ ـ ٢ ـ ١ ماذا يستطيع أن يفعل جدار الحماية؟:

يستطيع جدار الحماية أن يكون نافعًا في كل مما يأتي:

- تركيز الإجراءات الأمنية في نقطة واحدة (نقطة الالتقاء مع الإنترنت) وذلك أفضل من توزيعها بين نقاط مختلفة وأجهزة مختلفة.
- فرض السياسة الأمنية، فجدار الحماية أشبه بشرطي المرور فيما يخص استفادة المستخدمين من خدمات الإنترنت فيسمح بهذه الخدمات أو يمنعها تبعًا للسياسة الأمنية للشركة.
- تسجيل وقائع الاستخدام بدقة طالما أن كل الرسائل والأوامر تمر به عند خروجها إلى الإنترنت أو قدومها منها. ويستطيع جدار الحماية تسجيل كافة المعلومات عن حركة المرور هذه.
- الحد من درجة تعرض الشبكة للأخطار، وربما كانت هذه هي أهم الفوائد لحماية الشبكة الداخلية من أخطار الإنترنت، أو أحيانًا لحماية بعض أقسام الشبكة الداخلية من بعضها الآخر، وبذلك إذا تعرض جزء من الشبكة للأخطار يمكن منع انتشار هذه الأخطار في باقي أقسام الشبكة.

٩ ـ ٢ ـ ٢ ما لا يستطيع أن يفعله جدار الحماية:

ذكرنا من قبل أن جدار الحماية وحده لا يكفي لحماية الشبكة الداخلية، وإنما يجب أن تضم منظومة الأمن الشامل أجهزة أخرى تحدثنا عنها من قبل في هذا الكتاب، وهنا بعض الأمور التي لا يستطيع جدار الحماية أن يحققها:

- الحماية من مهاجمي الداخل، فطالما أن موقع جدار الحماية هو على حدود الشبكة فإنه لا يستطيع أن يفعل الكثير لمهاجم من الداخل يريد سرقة بعض المعلومات من أحد أجهزة الشبكة الداخلية، أو تخريب الأجهزة أو البرامج أو تعديلها، فإن ذلك سيتم بعيدًا عن (أعين) جدار الحماية، وعلى مسئولي الأمن اتخاذ إجراءات حماية أخرى. فماذا يفعل كلب الحراسة إذا كان الثعلب موجودًا داخل حظيرة الدجاج؟!

- الحماية من الاتصالات التي لا تمر عبر جدار الحماية، إذا سمح موقع ما بالاتصالبالإنترنت من خلال " مودم " مركب في أحد الأجهزة دون المرور بجدار الحماية، وهو ما نطلق عليه " الأبواب الخلفية ". فإذا تمكن أحد المستخدمين من تركيب مودم في جهازه والاتصال بالإنترنت فلا يستطيع جدار الحماية فعل شيء. فماذا يفعل كلب الحراسة إذا كان الباب الخلفي للحظيرة مفتوحاً لكافة الثعالب في المنطقة؟!

- الأخطار الجديدة تماماً والتي لم يصمم جدار الحماية مسبقًا للحماية منها، فجدار الحماية لا يستطيع التأقلم (فوريًا) لمواجهة أي سيناريو للأحداث يفاجأ به. ولذلك يهتم مسئولو أمن المعلومات بتحديث تهيئة جدران الحماية باستمرار لمواكبة ما يتم اكتشافه من أفكار جديدة. وإذا أصررنا على استخدام تشبيه كلاب حراسة الدجاج فماذا يفعل كلب الحراسة في مواجهة أخطار جديدة لم يتدرب عليها مثل خطر الحريق أو فساد العلف مثلاً.

- الحماية التامة من الفيروسات، فبرغم أن جدار الحماية يستطيع حجب الكثير من الفيروسات، إلا أن ذلك لا يتم بصورة كاملة تكفي للاستغناء عن اقتناء برنامج الحماية من الفيروسات. فلاكتشاف الفيروس ضمن حزمة بيانات مارة عبر جدار الحماية، فعليه أولاً أن يكتشف أن هذه الحزمة جزء من برنامج، ثم أن يحدد طبيعة هذا البرنامج، ثم عليه أن يكتشف أن هذا البرنامج قد تم تعديله بواسطة فيروس. ويزداد الأمر صعوبة مع ما تخضع له حزم الرسائل من ضغط (Compression) وتشفير (Encryption) ناهيك عن مصادر الفيروسات الأخرى مثل الأقراص الممغنطة أو تلك التي تستطيع أن تتفادى المرور بجدار الحماية. فلابد من وجود نظام لمكافحة الفيروسات ضمن منظومة الأمن الشامل. ألا يقف كلب الحراسة عاجزًا عن تفتيش ميكروب أو فيروس في حظيرة الدجاج؟!.

- التهيئة الذاتية.. فجدار الحماية يحتاج إلى من يقوم بتهيئته لأن كل موقع يختلف عن الموقع الآخر في طبيعته وسياسته الأمنية. ولذلك لا يمكن أن تشتري جدار حماية

(جاهزًا) يتـم تركيبه دون بذل جهد في تهيئته وتـدريبه، هذا فضـلاً عن الجـهد المبذول في اختياره من البداية، وإلا كان الأثر عكسيًا وأعطانا جدار الحماية إحساسًا زائفًا بـالأمان. وهذا ما نراه في جهات كثيرة نُدعـى إليها لتقديم الاستشارة الأمنية، وعند سؤالهم: هل لـديكم جدار حماية؟ يجيبون: طبعًا.. طبعًا! ولكن عند الفحص يتبين أن الجدار ملـيء بالثغـرات! ومرة ثـانية نـلجأ لمثال كلب الحراسـة الذي يجـب أن نبذل جهدًا في اختياره ثم في تدريبه وتهيئته للدور المطلوب منه.

٩ـ٣ أنواع جدران الحماية:

إذا أردنـا أن نصـنف جدران الـحمايـة فمن الأفـضل أن نصـنـفها وفـقًـا لأسلوب بنائهـا ووفقًا للتـقنية المسـتخدمـة فيها لـلـتحكم في المرور مـن خـلال الشبـكـة. لذلك نستطيع تصـنيف جدران الـحماية في نوعين رئيسـيين هما: "مصـافي حزم الرسائل" (Packet filters) وأجـهزة التفويض "بروكسي" (Proxy).

٩ـ٣ـ١ مصافي حزم الرسائل (Packet filters):

تصـفـية حزم الـرسائل (Packet filtering) هـو أحد الأسـاليب الناجـحة للتحكم في المرور عبـر الشبكة، فيقوم جدار الحماية من هذا الـنوع بمراجعة القواعد الأمنية المخزنة في ذاكرته عنـد التعامل مع كـل حزمة رسـائل تمر به. وتـخـتلـف أنواع جدران الـحـماية المتوفرة بالأسواق في كيفيـة تنفيذ هذه المهمة. فبينما يقوم بعضـها باستبدال ذلك الجزء من نظـام التشغيـل الذي يتولـى مهمة تمـرير الحزم استـبدالاً كاملاً، فـإن البعض الآخر يستخدم برامج يتم إلـحاقها بنظام التشغيل لتتولى مهمة اتخاذ قرار التمرير من عدمه.

هذا النوع من جدران الحماية إما أن يفحص بيانات الرسالة ذاتها أو يكتفي بفحص بعض الحقول في مقدمة الرسـالة (Header) [Escamilla ١٩٩٨] ومن بين الحقول التي يتم فحصـها بواسطة هذا النوع من جدران الحماية:

- مصدر الرسالة وجهة الوصول.
- المنفذ المستخدم (Port)
- نوع البروتوكول المستخدم (TCP, UDP,...)
- نوع الخدمة المؤداة (FTP, telnet, DNS, RIP)

ويتم تركيب " مصافي حزم الرسائل " عادة في إحدى صورتين: إما كموجه حاجب (Screening router) أو كحاسب منيع (Bastion host) وكلاهما يكون به أكثر من بطاقة شبكة " (Multi homed) الموجه الحاجب " هو عبارة عن جهاز حاسب مخصص للتحكم في مرور حزم الرسائل بين أقسام الشبكة، أو بينها وبين شبكة الإنترنت، بينما " الحاسب المنيع " هو عبارة عن جهاز حاسب عادي يتم (تقويته) عن طريق حذف أي برامج غير ضرورية، أو أي برامج قد تسبب إضعافًا لأمن الشبكة.

عند وصول رسالة، تستطيع هذه المصفاة تحديد أي بطاقة من بطاقات الشبكة قد استقبلت هذه الرسالة (دون النظر إلى محتوى الرسالة أو مقدمتها)، ومن ثم يتم فحص الرسالة بناء على المعلومات المسجلة في مقدمتها لمعرفة وجهتها ثم إرسالها إلى الوجهة الصحيحة. فإذا أردنا مثلاً منع كل الرسائل الواردة من شبكة الإنترنت باستثناء الرسائل الواردة من العناوين التي تبدأ بالعنوان (١,٢٢,٣٣٣)؛ فيمكن تهيئة الموجه ليقوم بهذه المهمة.

بالإضافة إلى حجب العناوين يمكن أيضًا منع حزم الرسائل التي يحدد مرسلها مسارًا معينًا لمرورها (Source routing) وهذا أحد أساليب المقتحمين (Hackers) لاستغلال بعض العناوين في اقتحام عناوين أخرى.

يمكن تقسيم هذا النوع من جدران الحماية إلى نوعين فرعيين هما: مصفاة الحزم الاستاتيكية (Static packet filter) ومصفاة الحزم الديناميكية (Dynamic packet filter).

٩ـ٢ـ١ـ١ مصفاة الحزم الاستاتيكية (Static packet filter):

يتحكم هذا النوع في تمرير الرسائل عن طريق استخدام المعلومات الموجودة في مقدمة الحزمة (Packet header)، وذلك بمقارنتها مع " قائمة التحكم في الاستخدام " (ACL) أو (Access Control List) المخزنة في المصفاة ومن ثم يتخذ قرار التمرير من عدمه. ولاتخاذ القرار الصحيح يتم فحص عنوان الجهة المرسلة، وعنوان الجهة المستقبلة، ورقم منفذ الخدمة، وحقل العلامات (TCP flags) الذي يبين طبيعة الرسالة. وهذا الحقل يحتوي على مجموعة من العلامات (Flags) التي قد تكون نشطة (=١) أو خاملة (= ٠). وعلامات هذا الحقل عندما تنشط تكون على النحو التالي:

(SYN) تستخدم هذه العلامة لبدء جلسة الاتصال، وبعد إرسالها لا يجب أن تنشط في أي وقت آخر خلال جلسة الاتصال.

(FIN) تشير هذه العلامة إلى أن النظام المرسل يود إنهاء جلسة الاتصال الحالية.

(ACK) تشير هذه العلامة إلى أن هذه الرسالة عبارة عن رد على طلب معلومات سبق إرساله إلى الخادم الذي يرسل الرد المحتوي على هذه العلامة النشطة.

(RST) تعيد هذه العلامة حالة جلسة الاتصال الحالية إلى الوضع الأصلي (Reset)، ويتم ذلك عادة في حالة حدوث فشل في عملية النقل لم يمكن التغلب عليه.

(URG) هذه العلامة تدل على احتواء الحزمة على معلومات ذات أولوية عالية (Urgent) مطلوب تمريرها على الفور، وعلى النظام المستقبل معالجة هذه الحزمة قبل أي بيانات أخرى قد تكون في الانتظار.

(PSH) مهمة هذه العلامة في حالة تنشيطها منع النظام المرسل من وضع البيانات في قائمة انتظار قبل إرسالها؛ فمعظم النظم المرسلة تضع البيانات في قوائم وذلك انتظاراً لمزيد من البيانات، وذلك بهدف تقليل عدد حزم الرسائل المرسلة.

ويلعب هذا الحقل (حقل العلامات) دوراً هاماً في مساعدة " مصفاة الحزم الاستاتيكية " على أداء مهمتها، لأنه من غير المعتاد أن نطلب من جدار الحماية منع كل

البريد الوارد من موقع معين، بل لابد أن تكون هناك شروط لهذا المنع، ومعظم هذه الشروط يمكن معالجته بفحص هذا الحقل. فقد تكون السياسة الأمنية هي مثلاً: " يسمح لكل المستخدمين باستخدام شبكة الإنترنت، ولكن تمنع أي رسائل واردة من شبكة الإنترنت ". ومن ثم لا بد للمصفاة عند استقبالها للرسائل الواردة من الإنترنت أن تتأكد أولاً أن هذه الرسالة ليست ردًا، أو استجابة، لطلب مرسل من الشبكة للإنترنت. فتقوم المصفاة بمنع كل الرسائل الواردة، ما عدا تلك الواردة كاستجابة. وتستطيع المصفاة معرفة نوع الرسالة الواردة، وهل هي استجابة أم لا، عن طريق اختبار حقل العلامات (TCP flags) والتأكد من أنه يحتوي على العلامة (ACK) في الحالة النشطة (ACK=١)، أي أن هذه الرسالة هي استجابة لطلب بيانات من الحاسب قد سبق إرساله.

ولذلك يطلق على " مصفاة الحزم الاستاتيكية " أنها مصفاة (غير ذكية) لأنها لا توفر إلا القليل من الحماية ضد الأنواع المتقدمة من الهجوم، إذ إنها لا تأخذ في الاعتبار سوى كمية محدودة من المعلومات وتكتفي بها لاتخاذ القرار بتمرير الحزمة أو منعها، ويتم تنفيذ التصفية الاستاتيكية عادة عن طريق الموجهات (Routers).

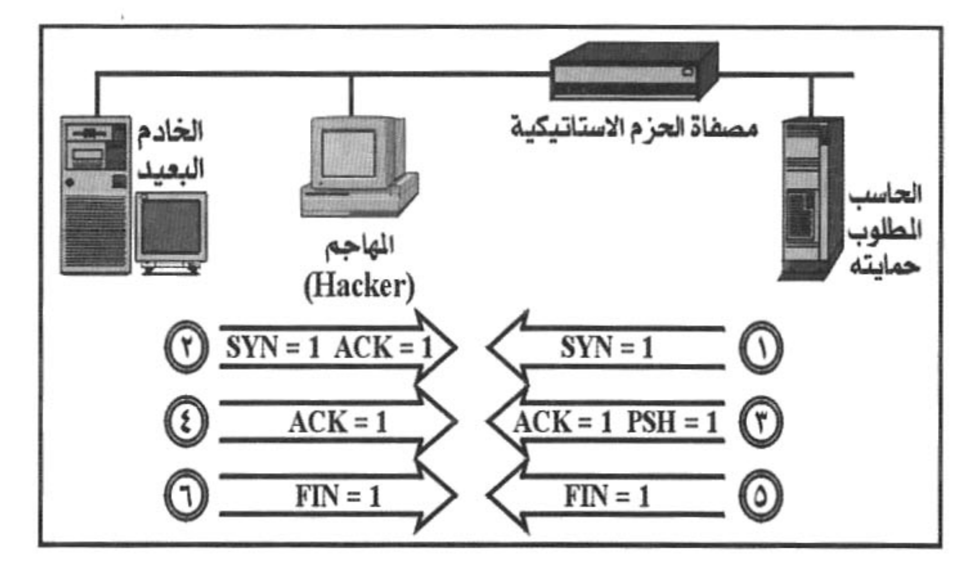
٩-٢-١-٢ مصفاة الحزم الديناميكية (Dynamic packet filter):

تتفوق " مصفاة الحزم الديناميكية " (Dynamic packet filter) عن المصفاة الاستاتيكية باحتفاظها " بجدول حالة " (State table) يمكنها من مراقبة حالة جلسة الاتصال، فهي لا تعتمد على محتويات حقل العلامات (TCP flags) وحده. ولتوضيح أهمية هذا الفارق نفترض أن أحد المهاجمين أرسل حزمة بيانات للنظام في محاولة للتسبب في حدوث انهيار للنظام. هذا المهاجم يمكن أن يقوم بحيلة لخداع المصفاة، وذلك بأن يجعل علامة (ACK) في حقل العلامات في الوضع النشط (ACK=١) لكي يجعل الرسالة تبدو وكأنها استجابة لطلب أحد المستفيدين بالشبكة الداخلية. المصفاة الاستاتيكية يمكن أن تنخدع بهذه الحيلة، ولكن المصفاة الديناميكية عند استقبال هذه

الحزمة تقوم بمراجعة جدول الاتصال أو " جدول الحالة " ، وعندئذ ستكتشف المصفاة أنه لم يحدث أي اتصال مسبق مع هذا الموقع الذي وردت منه الرسالة.

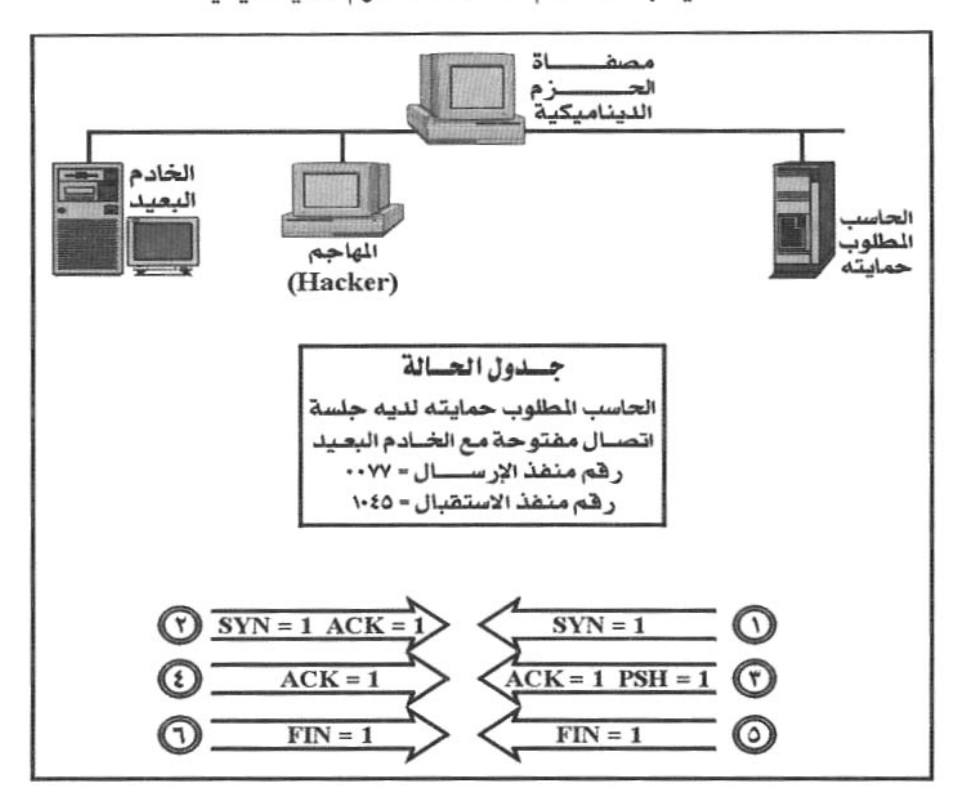
يوضح الشكلان (٩-٢) و (٩-٣) الفرق بين الحماية باستخدام مصفاة الحزم الاستاتيكية والمصفاة الديناميكية.

شكل (٩-٢)
الحماية باستخدام مصفاة الحزم الاستاتيكية



شكل (٩-٣)

الحماية باستخدام مصفاة الحزم الديناميكية



في الحالتين تحتوي " قائمة التحكم في الاستخدام " (ACL) والمخزنة في أي من المصفاتين على القواعد التالية:

(١) السماح للحاسب المطلوب حمايته بإقامة أي جلسة اتصال مع الخادم البعيد للاستفادة من الخدمات التي يقدمها.

(٢) السماح بمرور الحزم التابعة لأي جلسة اتصال سبق إقامتها.

(٣) منع أي رسائل أخرى لا تحقق الشرطين السابقين.

وفـقًا للقاعـدة الأولى يتـم السماح لـلحاسب المطلـوب حمايتـه ببدء جلسـة اتصـال مـع الخـادم البعيـد، ويعني ذلك أن الحـزمـة التـي تحتوي علـى علامـة (SYN) نـشطة (SYN=١) والتي تعني بدء جلسـة الاتصـال يسمح لها بالمرور إذا كـان مصدرهـا هو الحـاسب المطلـوب حمايته وإذا كانت جهـة الوصـول هي الخـادم البعيد، وذلك للسماح بكل أنواع الاستخدام للخدمات المتاحة على ذلك الخادم البعيد.

ووفقًا لـلقاعـدة الثـانيـة يتـم السمـاح بمرور كـافة الحـزم التي لا تـوجد بهـا علامة (SYN) نشـطة (SYN=٠)، ممـا يدل علـى أنـهـا رسـائل تـابعـة لجلسـة اتصـال سبق إقامتها.

والقاعـدة الثالثة تعـني أن أي اتصال لا ينتمي بـوضـوح لإحدى القاعـدتين السابقتين يجب منعه.

يَستـخـدم كل مـن جداري الـحمايـة في الشكـل (٩-٢) والشكل (٩-٣) أي المـصفاة الاسـتاتيكيـة والمصفاة الـديناميكيـة نفس القـواعد، ولكن يـكون الاختلاف فيمـا لدى كل منهمـا من معلومات إضافية يبني على أسـاسـها قراره بالمرور. ويتضـح من الشكلين أن الحـاسـب المطلـوب حمـايته يبـدأ جلسـة اتصـال مع الخـادم البعيـد (SYN =١) ويتم التعارف (SYN =١ , ACK =١)، ثم يطلـب الحـاسب بعض البيانـات من الخادم البعيد (ACK =١ , PSH =١)، الـذي يرد علـيه بالبيـانات المطلـوبة (SCK =١)، ثـم يتم إنهـاء جلسة الاتصـال بطلب من الحـاسب (FIN =١) وموافقة من الخـادم البعيد (FIN =١).

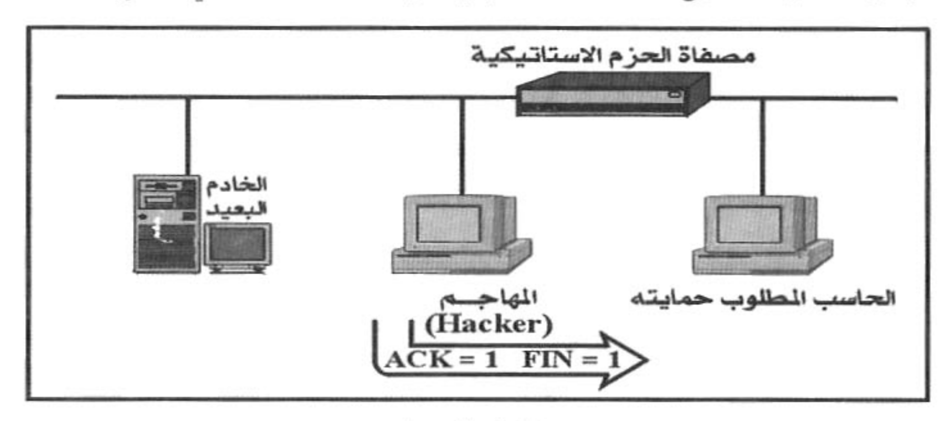
المصفـاة الاسـتـاتـيكيـة في شكـل (٩-٢) لا تـنظـر إلا إلـى حقل العلامـات (Flags) للتحقق مـن عدم وجود علامة (SYN) نشطة أي (SYN=١) دليلاً علـى أن هذه الحزمة جـزء من جـلسـة اتصـال قـائمـة بـالفعـل، ومن ثم تـسمح لـهـا بـالمرور. أمـا المصفـاة الديناميكية في شكل (٩-٣) فهـي تفعل الشيء نفسه ولكن مع إنشاء سجل في " جدول الحـالة " (State table) عند بـدء الجلسة، وفي كل مرة يحاول الخـادم البعيد الاستجابة للحاسب المطلوب حمايته تقوم المصفاة الديـناميكية بمراجعة " جدول الحـالة " للتأكد من

أن الحاسب قد أرسل بالفعل في طلب بيانات من الخادم، وكذلك للتأكد من رقم منفذ الإرسال ورقم منفذ الاستقبال في جدول الحالة، وأنهما يطابقان الأرقام ا لواردة في حزمة البيانات المارة. كما تراجع المصفاة الديناميكية رقم الحزمة المتسلسل ورقم التعارف، ولا تسمح بمرور الحزمة إلا بعد تطابق كل هذه البيانات. وبمجرد ورود الحزمة التي تحمل علامة (FIN) في الحالة النشطة (FIN=١) لإنهاء الجلسة يتم حذف السجل الذي يحتويه " جدول الحالة "، وهذا السجل يتم حذفه كذلك إذا انقضت مدة معينة دون رد من أحد الطرفين (مما يعني أن خطأ ما قد حدث).

إذا حاول مهاجم خداع أو مهاجمة الحاسب فعليه أولاً أن يرسل إليه حزمة بها علامة (SYN) نشطة ($\overrightarrow{\text{SYN =١}}$) لبدء جلسة اتصال مع الحاسب، وهذه الخدعة لن تجوز على المصفاتين (الاستاتيكية والديناميكية) لأن من المفروض أن هذه العلامة تكون هي وحدها النشطة في حقل العلامات إذا كانت آتية من الحاسب الداخلي إلى الخارج ($\overleftarrow{\text{SYN =١}}$) وليس العكس. وفي حالة ورودها من الخارج إلى الداخل فلابد أن تكون مصحوبة بعلامة (ACK) نشطة أي (ACK=١)، لأن الحاسبات في الشبكة الداخلية هي التي تطلب خدمات المواقع البعيدة وليس العكس. وستفطن كلا المصفاتين لهذا الخطأ وتحجب الرسالة. تحسبًا لذلك سيقوم المهاجم بإرسال حزمة بها علامةFIN نشطة وعلامة ACK نشطة ($\overrightarrow{\text{FIN =١ , ACK =١}}$). هذه الحزمة ستخدع المصفاة الاستاتيكية التي تأكدت فقط من عدم وجود علامة (SYN)النشطة وستسمح بمرور رسالة المهاجم، أما المصفاة الديناميكية فعند اكتشافها لعدم وجود علامة(SYN) نشطة ستقوم بمراجعة " جدول الحالة " وهنا ستكتشف عدم وجود جلسة اتصال قائمة مع المهاجم، ومن ثم تكتشف أنه لا يوجد مبرر لمحاولة إنهاء جلسة لم توجد أصلاً، وستكتشف أن الجلسة المفتوحة هي مع الخادم البعيد وليس مع المهاجم كما يوضح الشكلان (٩-٤) و(٩-٥).

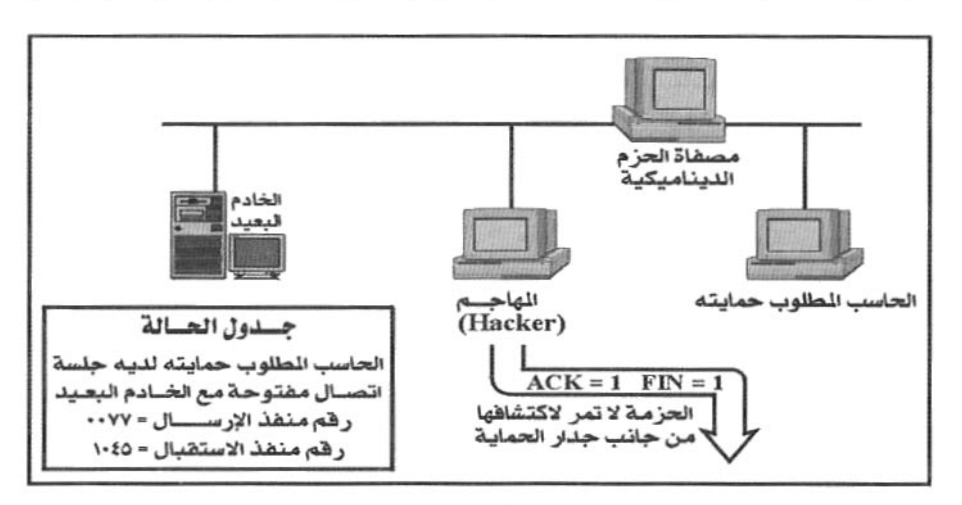
شكل (٩-٤)

جدار الحماية من نوع المصفاة الاستاتيكية حيث تمر الحزمة التي تخدع المصفاة



شكل (٩-٥)

جدار الحماية من نوع المصفاة الديناميكية لا ينخدع من جانب المهاجمين



والآن ما الذي يجب على المهاجم أن يفعله حتى يخدع جدار الحماية من نوع المصفاة الديناميكية؟ على هذا المهاجم أن يقوم بما يلي:

- انتحال العنوان (IP address) الخاص بالخادم البعيد.

- تحييد الخادم البعيد لضمان ألا يرسل من جانبه أي استجابات للحاسب المطلوب

اختراقه خلال الجلسة.

- إيجاد وسيلة لاستقبال الحزم المرسلة من الحاسب المطلوب اختراقه وقراءتها ليستطيع التصرف على هذا الأساس.
- معرفة منفذ الإرسال ومنفذ الاستقبال المسجلين في " جدول الحالة ".
- انتحال أرقام التسلسل (Sequence numbers) وأرقام التعارف (Acknowledgment numbers) للحزم المتبادلة.
- تنفيذ كل ما سبق بسرعة كبيرة تفاديًا لتجاوز الفترة الزمنية المسموح بها (Timeout).

ويتضح من ذلك أنه برغم أن هذه الخطوات السابقة ليست مستحيلة التنفيذ من جانب المهاجم، إلا أنها تجعل الأمور صعبة عليه، وهي تتطلب مهاجمًا فذًا، كما تتطلب أن تكون الغنيمة باردة، أي تستحق كل هذا العناء.

مما سبق يتضح أن هذا النوع من جدران الحماية (مصفاة الحزم الديناميكية) يمكن استخدامه لحماية الشبكة الداخلية (ننصح بالبعد عن المصفاة الاستاتيكية)، ولكن يعيب هذا النوع أنه لا يبني أحكامه على محتويات الحزمة ذاتها، وإنما يبنيها فقط على أساس ما تحتويه مقدمة الحزمة " وجدول الحالة " الذي يحتفظ به. أما إذا أردنا حكمًا أكثر دقة مبنيًا على محتويات حزمة الرسائل ذاتها فعلينا أن نلجأ إلى النوع الثاني من أنواع جدران الحماية وهو جهاز التفويض " بروكسي " (Proxy).

٩-٣-٢ خادم البروكسي (Proxy server):

جهاز " التفويض " (Proxy)، وسوف نطلق عليه اسم " خادم البروكسي "، هو أحد أنواع جدران الحماية القوية، وهو يتولى طلب خدمات الإنترنت من الشبكة نيابة عن المستفيد، مثل نقل الملفات (FTP)، أو الدخول عن بعد (Telnet)، ومن ثم فهو يعمل كبوابة بين المستفيد والإنترنت. ولذلك يطلق على هذا النوع من جدران الحماية اسم

"بـــوابـــة الـتـطـبـيـقـــات" (Application-level gateway) [Zwicky ٢٠٠٠] أو (Application gateway) [Brenton ١٩٩٩].

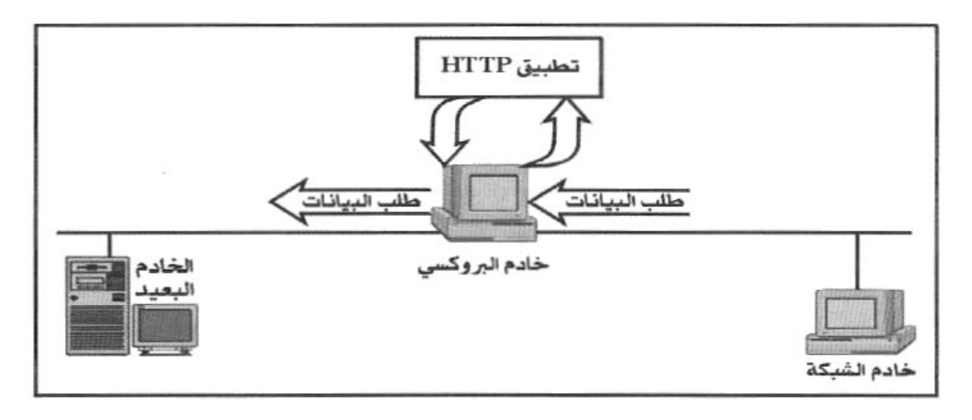
وهو قد يستخدم كجدار حماية بدلاً من أسلوب تصفية حزم الرسائل، وباستخدام خادم البروكسي لا يتم الاتصال بين مرسل الرسالة ومستقبلها مباشرة أبداً وإنما يلعب خادم البروكسي دور الوسيط بينهما.

على العكس من المصافي الديناميكية والاستاتيكية فإن خادم البروكسي لا يقوم بتوجيه حزم الرسائل، ولكنه يتفاهم مع كل طرف ممثلاً للطرف الآخر، وكأنه المترجم يقوم بالترجمة بين زعماء الدول فيتوجه كل زعيم بحديثه إلى المترجم الذي يقوم بترجمته للزعيم الآخر باللغة التي يفهمها.

يبين الشكل (٩-٦) قيام خادم البروكسي بدور الوسيط، حيث يرغب هنا حاسب الشبكة في طلب إحدى صفحات النسيج (Web page) من الخادم البعيد، فيقوم بصياغة الطلب وإرسال المعلومات المطلوبة إلى خادم البروكسي الذي يعتبر البوابة المؤدية إلى الشبكة البعيدة.

شكل (٩-٦)

خادم البروكسي يقوم بدور الوسيط



بمجرد استلام خادم البروكسي لطلب البيانات فإنه يقوم بتحديد نوع الخدمة

المطلوبة من جانب خادم الشبكة ويحدد التطبيق المستخدم ويمرر إليه الطلب. في المثال المبين في الشكل (٩-٦) كان المطلوب هو إحدى صفحات النسيج، ومن ثم تم توجيه الطلب إلى تطبيق (HTTP) وهو عبارة عن برنامج يتم تنفيذه في ذاكرة خادم البروكسي، والمهمة الوحيدة التي يتخصص فيها هذا البرنامج هي التعامل مع (HTTP) عند استلام (تطبيق HTTP) لطلب البيانات يقوم بمراجعة " قائمة التحكم في الاستخدام " (ACL) للتأكد من السماح لهذا النوع من الرسائل بالمرور، وعند التأكد من ذلك يقوم خادم البروكسي بصياغة طلب جديد يقوم بإرساله إلى الخادم البعيد وكأن هذا الطلب مرسل من خادم البروكسي وليس من خادم الشبكة. ولذلك فعندما يقوم الخادم البعيد بالرد فإنه يرد على خادم البروكسي، الذي يقوم بدوره بتمرير الرد إلى (تطبيق HTTP) الذي يراجع البيانات الواردة، ثم يقوم خادم البروكسي بإنشاء حزمة رسائل جديدة ويمررها إلى خادم الشبكة. ويتضح أن طرفي الاتصال لا يتصلان ببعضهما مباشرة وإنما يتم ذلك من خلال خادم البروكسي للتأكد من أن كل شيء على ما يرام.

يجد خادم البروكسي نفسه في وضع يسمح له بحجب بعض الرسائل في أي اتجاه، فيستطيع مثلاً أن يتأكد من أن خادم الشبكة يستخدم كخادم للقراءة فقط من خارج الشبكة، وذلك عن طريق منع الرسائل القادمة من خارج الشبكة إلى خادم البروكسي إذا كانت تحاول الكتابة أو تعديل البيانات على خادم الشبكة.

٩-٣-٢ استخدام الأجهزة كجدران حماية (Firewall appliances):

توجد في الأسواق أجهزة تستخدم كجدران حماية (Firewall appliances) تقوم بكل مهام جدار الحماية، وهي تناسب الشركات الصغيرة أو الشركات التي لا تستطيع تعيين مسئول أمن معلومات خبير بإدارة جدران الحماية من الأنواع السابقة [Ogletree ٢٠٠٠]. وتتمتع هذه الأجهزة بسرعة وسهولة التركيب، وواجهة استخدام سهلة، إذ يوجد جهاز واحد يحتوي على كل شيء. وهي تعمل

مع كافة أنواع الاتصال كالاتصال بخطوط المراقمة (Dial-up) أو خطوط " إيثرنت " أو حتى الخطوط من مستوى (T١).

توجد في هذه الأجهزة سياسات أمنية جاهزة، فلا يحتاج المستخدم أن يفهم كثيرًا من التفاصيل، ويمكنها أن تعمل بأسلوب تصفية الحزم أو بوابة التطبيق (خادم البروكسي)، كما تستطيع أن تؤدي خدمة ترجمة عناوين الشبكة (NAT) أو (Network Address Translation) تخرج هذه الأجهزة تقارير سهلة المتابعة، وهي قادرة على إصدار الإنذارات في حالة الشك في رسالة معينة. كما أن لديها القدرة على التعامل مع الشبكات الخاصة الافتراضية (VPN)، كما يمكن الاستفادة من خدمات الشركة الموردة. وسنقدم خلال القسم التالي من هذا الفصل (٩ ـ ٤ ـ ٥ ، ٩ ـ ٤ ـ ٦) تقييمًا لهذا النوع من جدران الحماية.

٩ـ٤ مقارنة أنواع جدران الحماية:

في هذا القسم سنقوم بإجراء العديد من المقارنات بين الأنواع المتاحة من جدران الحماية. كما سنقوم بالمقارنة بهدف اتخاذ قرار الشراء أم التركيب، وقرار استخدام جهاز (Hardware) كجدار حماية أم برمجيات (Software) يتم تشغيلها على جهاز حاسب عادي، وكذلك دراسة بيئة التشغيل المناسبة لجدران الحماية.

٩ـ٤ـ١ مزايا مصافي حزم الرسائل:

يمتاز هذا النوع من جدران الحماية بعدة مزايا يمكن تلخيصها فيما يلي:

(١) يمكن حماية شبكة كاملة باستخدام موجه حاجب (Screening router) واحد عن طريق وضعه في المكان المناسب من الشبكة (عند التقاء الشبكة الداخلية بشبكة الإنترنت).

(٢) الكفاءة العالية للمصفاة البسيطة، فهنا تكمن الميزة في البساطة؛ لأن ذلك يعني

تركيز الاهتمام في عدد محدود من مقدمات الحزم (Headers)، مما يعني عبئًا (Overhead) أقل على نظام التشغيل بعكس استخدام خادم البروكسي الذي يعني فحص محتويات الرسائل [Zwicky ٢٠٠٠].

(٣) الانتشار الواسع لهذا النوع وتعميم استخدامه في العديد من المنتجات يجعل من السهل العثور على الخبرات اللازمة لإدارته وتشغيله، والاطمئنان على إمكان وجوده في المواقع المختلفة وفي الدول المختلفة التي تقع بها فروع الشركة.

٩ـ٤ـ٢ عيوب مصافي حزم الرسائل:

هناك بعض العيوب لهذا النوع من جدران الحماية نوجزها فيما يلي:

(١) أدوات التصفية المتوفرة حاليًا ليست على درجة عالية من الكفاءة؛ فالقواعد الموضوعة للرسائل المطلوب مراقبتها من الصعب تطبيقها، ومن الصعب اختبارها للتأكد من عملها بكفاءة، وقدرات هذا النوع من جدران الحماية تعتبر غير كاملة فهي لا تمنع كل أنواع الاقتحام، والأهم من ذلك وجود عيوب (Bugs) في العديد من البرمجيات المستخدمة في هذا النوع. في حالة وجود عيب في خادم البروكسي فإنه ببساطة يتوقف عن العمل بينما تستمر مصفاة الحزم في العمل في حالة وجود العيب مما يعني ثغرة أمنية خطيرة.

(٢) تحد مصفاة الحزم من كفاءة الموجه (Router)، فعملية التصفية للحزم تلقي بعبء إضافي على الموجه، خاصة إذا تعارضت القواعد المتبعة للتصفية مع بعض أساليب تحميل المعلومات في الذاكرة الخبيئة (Caching) فمثلاً في حالة استخدام وظيفة (Fast-path) في أجهزة شركة " سيسكو " (Cisco) يتم تنفيذ وظائف التوجيه الأساسية بالكامل من خلال بطاقة الشبكة (Network card)دون تدخل المعالج (CPU)، ولكن تنفيذ بعض قواعد التصفية يتطلب تدخل المعالج لفحص كل حزمة مما يسبب بطئًا في الأداء.

(٣) لا يمكن بسهولة فرض سياسات معينة مع بعض الموجهات التي تنفذ أسلوب

تصفية الحزم، فهذه الموجهات لا تحتفظ بالمعلومات المطلوب استخدامها لتنفيذ السياسة الأمنية. فمقدمة الحزمة مثلاً تبين بوضوح الجهة المرسلة (Host) ولكنها لا تبين شخصية المرسل من داخل هذه الجهة، ومن ثم لا يمكن وضع أي نوع من القيود على الرسائل الصادرة من مستخدم معين، والأمر نفسه عند تحديد منفذ الاستقبال فيتم تحديد جهة الوصول وليس الشخص المفروض أن تصل إليه الرسالة. ويفتح هذا العيب الباب واسعًا أمام المقتحمين من الداخل للعبث بالرسائل. ولذلك تفرض بعض مصافي الحزم على المستخدم تعريف نفسه بدقة قبل إرسال الحزم، ومن ثم يمكن تصفية هذه الحزم وفقًا لاسم المستخدم. وإن كان ذلك يستبعد ميزة الشفافية التي كانت تحسب لهذا النوع من جدران الحماية.

٩-٤-٣ مزايا استخدام خادم البروكسي:

لاستخدام خادم البروكسي (Proxy server) كجدار حماية عدة مزايا من بينها:

(١) يستخدم هذا النوع بشكل جيد في تسجيل وقائع الاستخدام (Logging)، ذلك لأن خادم البروكسي يستطيع فهم بروتوكولات التطبيق. فمثلاً بدلاً من تسجيل جميع حزم الرسائل المارة، فإن خادم البروكسي المتخصص في نقل الملفات (Proxy server FTP) يقوم فقط بتسجيل الأوامر المتبادلة بين الشبكة والخادم البعيد مما يؤدي إلى ترشيد استخدام سجل الوقائع وتوفير الوقت.

(٢) يقدم خادم البروكسي إمكانية استخدام الذاكرة الخبيئة (Caching) بالاحتفاظ بنسخة من طلبات البيانات، وذلك لأن جميع هذه الطلبات تمر عن طريق خادم البروكسي، وبالتالي إذا تكررت هذه الطلبات بشكل ملحوظ فإن الأداء يتحسن بشكل كبير.

(٣) يقوم خادم البروكسي بالتصفية بشكل أكثر كفاءة وأكثر ذكاء لأنه يفحص المحتوى، فهو أكثر قدرة على تصفية حزم (HTTP) على أساس نوع المحتوى، فيقوم مثلاً بمنع بعض برامج " جافا " أو " جافا سكريبت "، كما أنه أكثر قدرة من مصافي

الحزم على كشف الفيروسات.

(٤) يستطيع هذا النوع من جدران الحماية تحديد شخصية المستخدم لأنه يتدخل في كل العمليات المارة به، ومن ثم يستطيع اتخاذ الإجراءات التي تتوقف على شخصية المستخدم. وهذه العملية تتم في حالة خادم البروكسي بشكل أكثر سهولة من مصافي الحزم.

(٥) يعالج هذا النوع حالات الخطأ في توليد الحزم من نوع (IP)، لأنه يكون موجوداً في موقع متوسط بين العميل وبين شبكة الإنترنت، ومن ثم فهو يقوم بتوليد حزم (IP) جديدة تحل محل تلك التي قام العميل بتوليدها، وبذلك يعالج أي خطأ قد يحدث من جانب العميل عند توليد هذه الحزم ولا ينخدع بها.

٩-٤-٤ عيوب استخدام خادم البروكسي:

لا يمنع تعدد مزايا خادم البروكسي من وجود العديد من العيوب فيه، ومن هذه العيوب:

(١) تأتي معالجة الخدمات من جانب خادم البروكسي متأخرة عن ظهور هذه الخدمات التي تقدم على شبكة الإنترنت؛ فلابد من مرور فترة بين ظهور خدمة جديدة ومعالجة خادم البروكسي لها، فخادم البروكسي يعالج الخدمات القديمة المعروفة مثل خدمات نقل الملفات (FTP) والدخول عن بعد (Telnet)، أما ظهور خدمة جديدة فيحتاج إلى وقت حتى تتم إعادة برمجة خادم البروكسي ليستطيع التعامل مع هذه الخدمة، ويعتمد طول هذا الوقت أو قصره أساساً على تصميم هذه الخدمة ومدى مناسبتها للمعالجة من جانب خادم البروكسي، الأمر الذي يجعل الاستخدام الآمن للخدمات الجديدة غير ممكن بشكل فوري من جانب المواقع المختلفة، إلى أن تتوفر خدمة البروكسي المقابلة. ووجه الخطورة هنا يكمن في أن الشركة التي تريد استخدام هذه الخدمة ستضطر لوضعها خارج نطاق خادم البروكسي حتى تستطيع الاستفادة منها، مما يشكل ثغرة أمنية. وقد ظهرت مؤخراً خدمة خاصة تسمى (Generic proxy) تعالج هذا الأمر بعض الشيء.

(٢) قد يحتـاج خادم البروكسي خادمًا خاصًا لكل خدمة من الخدمات (لكل بروتوكول)، وذلك لأن خادم البروكسي قد يحتاج إلى فهم البروتوكول حتى يتمكن من اتخاذ القرار المناسب بتمرير الحزمة أو حجبها، ومن أجل أن يستطيع التنكر في صورة العميل في مواجهة الخادم البعيد ويتنكر في صورة الخادم البعيد في مواجهة العميل (الحاسب المطلوب حمايته). ويشكل تعدد الخوادم وتهيئتها وإدارتها عبئًا غير يسير، إلا في حالة استخدام خدمة (Generic proxy) التي ذكرناها في الفقرة السابقة، ولكننا في هذه الحالة نكون أقرب إلى مصافي الحزم منا إلى خوادم البروكسي!

(٣) في كثير من الأحيان يتطلب استخدام خادم البروكسي إدخال تعديلات على أداء المستفيد وعلى عمل التطبيقات وعلى الإجراءات المتبعة، باستثناء تلك الخدمات المصممة أصلاً للاستخدام مع خادم البروكسي. وربما تسبب هذه التعديلات عيوبًا أخرى، أو تشكل عبئًا على المستخدم وعلى كفاءة تشغيل النظام.

٩-٤-٥ مزايا استخدام الأجهزة كجدران حماية:

تحدثنا عن الأجهزة التي تستخدم كجدران حماية (Firewall appliances)، تلك التي تناسب الشركات الصغيرة أو الشركات التي لا تستطيع تعيين مسئول أمن معلومات خبير، وتتمتع هذه الأجهزة بالمزايا التالية:

(١) **سرعة وسهولة التركيب**: وتعتبر هذه ميزة هائلة لهذا النوع من جدران الحماية، فيمكن لمسئول الشبكة تركيب كابل الشبكة مباشرة في أحد مداخل الجهاز، وتركيب الخط المتصل بشبكة الإنترنت في المدخل الآخر. ثم عليه أن يجيب عن بعض الأسئلة البسيطة اللازمة لتهيئة الجهاز. ولا يحتاج الأمر إلى خبرة مسبقة من جانب المستخدم، ولا تستغرق عملية التركيب بالكامل أكثر من ساعة واحدة.

(٢) **واجهة استخدام سهلة**: إدارة هذا الجهاز سهلة إلى حد كبير، بل إن بعض هذه الأجهزة لا يوجد بها جهاز مراقبة (Monitor)، ويمكن تشغيل الأجهزة الحديثة عن

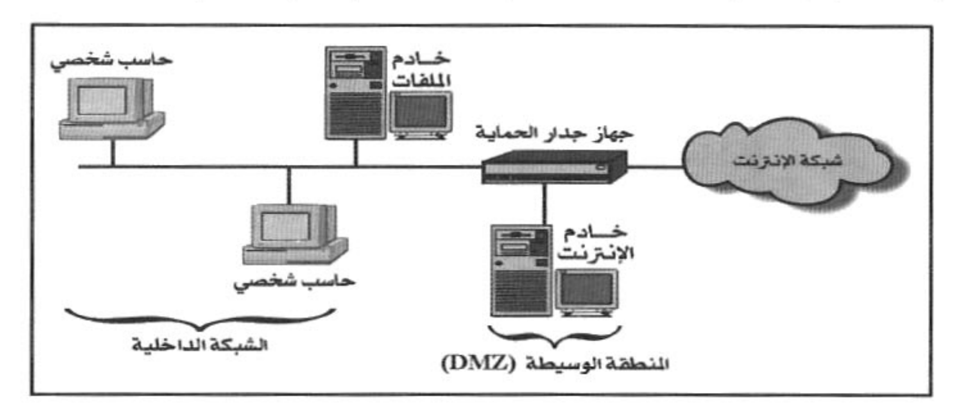
بعد، وذلك باستخدام واجهة رسومية، ولكن في هذه الحالة يجب أن تكون قناة الاتصال بين جهاز الحماية وجهاز المراقبة (Console) قناة مشفرة. ويتم التعامل مع جهاز المراقبة باستخدام الفأرة (Mouse) لتنفيذ معظم العمليات مثل إخراج التقارير، حيث يقوم مستخدم الجهاز باختيار التقرير المطلوب من قائمة تحتوي على اختيارات عديدة لأنواع مختلفة من التقارير.

(٣) **جهاز واحد يحتوي على كل شيء:** من بين المزايا المهمة لهذا النوع من جدران الحماية أن جهازًا واحدًا يضم كل شيء، وحجمه ربما يكون أصغر من حجم الحاسب الشخصي. وعادة يتم تشغيل هذا الجهاز باستخدام أحد نظم التشغيل المعروفة أو نظام تشغيل معدل بحيث يدعم وظائف جدار الحماية. وعادة يتم استخدام قرص مضغوط (CD ROM) يحتوي على نظام التشغيل، وذلك بهدف منع محاولات تعديل نظام التشغيل بواسطة المقتحمين (Hackers)، وبعض هذه النظم يعتبر مغلقًا تمامًا ويحتفظ بنظام التشغيل في ذاكرة الجهاز إلى جانب نظام جدار الحماية. وهذه البساطة هي أحد العوامل التي ترجح كفة نظام على الآخر.

(٤) **يعمل مع كافة أنواع خطوط الاتصال:** تعمل هذه الأجهزة مع كافة خطوط الاتصال مثل الخطوط المراقمة (Dial-up)، والشبكات الرقمية للخدمات المتكاملة (ISDN)، أو خطوط المشتركين الرقمية (DSL)، بل إن بعض الأجهزة الحديثة يمكنها العمل مع خطوط (T١)، وذلك دون الحاجة إلى أجهزة وسيطة لتوصيلها بهذه الخطوط. ويوجد في بعض الأجهزة وصلة إضافية تسمح بتركيب " خادم الإنترنت " (Web server) في المنطقة الوسيطة (DMZ) أو(Demilitarized zone) التي تقع بين الشبكة الداخلية وشبكة الإنترنت كما يبين الشكل (٩-٧). وهذه ميزة مفيدة للشركات التي تقتني خادم الإنترنت الخاص بها، برغم أن التوجه الحالي لبعض الشركات الصغيرة هو الاعتماد على خادم الإنترنت الموجود لدى مقدم الخدمة (ISP) ولكننا نرى أن اقتناء هذه الشركات لخادم إنترنت خاص بها لن يشكل عبئًا فنيًا كبيرًا لإدارته.

شكل (٩-٧)

بعض الأجهزة التي تعمل كجدران حماية بها مدخل إضافي لخوادم منطقة (DMZ)



(٥) **سياسات أمنية جاهزة:** لا تحتاج هذه الأجهزة إلى خبرة مسبقة لوضع سياسة أمنية معينة، فهي تحتوي على برامج مساعدة تسهل تهيئة جدار الحماية، مما يجعل عملية تركيب الجهاز سهلة وسريعة. وبهذه الأجهزة عدة سياسات أمنية جاهزة للاختيار من بينها، فيستطيع المستخدم اختيار السياسة الأمنية التي يريدها من ضمن قائمة الاختيارات، وبناءً على هذا الاختيار يقوم البرنامج المساعد (Wizard) بتهيئة الجهاز. بل إن بعض هذه الأجهزة يتيح إنشاء عدة سياسات أمنية مختلفة يمكن تخصيص كل منها لقسم من أقسام الشبكة.

(٦) **وظائف تصفية الحزم وخادم البروكسي:** تستطيع هذه الأجهزة أن تقوم بالوظيفتين معًا: وظيفة تصفية الحزم (Packet filtering) ووظيفة خادم البروكسي (Application proxy) للتحكم في الخدمات المقدمة من الإنترنت للشبكة الداخلية. ويتم تقديم هذه الخدمات بشكل شفاف، بمعنى أن المستفيد لا يحس بتدخل جدار الحماية في تقديم هذه الخدمات.

(٧) **وظائف ترجمة عناوين الشبكة:** هذه الوظيفة (NAT) أو (Network Address Translation) تمكن جهاز الحماية من التأقلم مع أي نظام عنونة يتبعه مقدم

الخدمة، وإذا كان لدى الشركة التي تقتني الجهاز مجموعة فرعية من العناوين فإن هذا الجهاز سوف يمكنها من تحديد عنوان الجهاز الفرعي على الشبكة الداخلية. فلابد أن يكون جهاز جدار الحماية قادرًا على ترجمة العناوين (NAT) لتستطيع الشبكة الداخلية الاتصال بشبكة الإنترنت.

(٨) **إخراج التقارير والإنذارات:** يعتبر إخراج التقارير سهلة الفهم وسهلة المتابعة وإصدار الإنذارات الواضحة من الأمور الضرورية للشركات التي ليس لديها خبراء متخصصون في أمن المعلومات. ولذلك تمتلك هذه الأجهزة القدرة على إخراج تقارير بالصورة التي يحددها المستخدم مسبقًا ومن ثم يستطيع المستخدم طلب تقارير أكثر تقدمًا وإحصاءات أكثر أهمية كلما زادت معلوماته وقدراته. وتمتلك هذه الأجهزة أيضًا القدرة على الإنذار عند حدوث وقائع مثيرة للشك أو احتمال حدوث اقتحام للشبكة وذلك بإرسال رسالة بريد إلكتروني لمسئول الشبكة أو مسئول الأمن.

(٩) **القدرة على التعامل مع الشبكات الخاصة الافتراضية:** تحتاج كثير من الشركات أن يتصل بها بعض موظفيها عن بعد، أو تتصل هي بفروعها البعيدة من خلال شبكة خاصة افتراضية (VPN) أو (Virtual Private Network) لتفادي استخدام خطوط اتصال خاصة مكلفة. وهذه الشبكة الخاصة التي تتم من خلال قنوات اتصال مشفرة تحتاج إلى أجهزة جدران حماية تستطيع التعامل معها، بحيث يتم تركيب هذه الأجهزة لدى فروع الشركة المختلفة (في أطراف الشبكة الخاصة الافتراضية).

٩-٤-٦ عيوب استخدام الأجهزة كجدران حماية:

(١) **عدم القدرة على كشف الانتهاكات المعقدة:** العيب الأساسي في استخدام الأجهزة كجدران حماية يكمن في بساطة هذه الأجهزة وعدم قدرتها على كشف الانتهاكات المعقدة.

(٢) **عدم المرونة:** من عيوب استخدام الأجهزة كجدران حماية هو عدم المرونة التي

تقدمها الأنواع الأخرى من جدران الحماية التي تستخدم البرامج والتي تتيح مرونة أكبر لمسئول أمن المعلومات في تحديد وتنفيذ السياسة الأمنية ومن ثم تعديلها.

(٣) **عدم الاحتفاظ بالمعلومات السابقة:** من بين العيوب كذلك أن أجهزة جدران الحماية لا توفر أو تحتفظ بالمعلومات السابقة، كما أنها لا تعطي تفصيلات للعمليات التي تمت على النظام باعتبارها أجهزة لا تتضمن برامج تفصيلية ولا تتمتع بما تتمتع به برامج جدران الحماية التي تتولى عملية التوثيق ومتابعة العمليات على الأنظمة واستخراج التقارير المطلوبة حسب الطلب.

(٤) **عدم توفر المزايا في جميع الأجهزة:** لا تتوفر المزايا العديدة التي ذكرناها لهذه الأجهزة في جميع الأجهزة، بل يجب التدقيق في الوثائق المصاحبة لهذه الأجهزة للتأكد من توافر المزايا التي تركز عليها الشركة التي تفكر في اقتناء هذا الجهاز.

٩-٤-٧ أي بيئات التشغيل أنسب لجدران الحماية؟:

سؤال يتردد كثيرًا: وهو أي بيئات التشغيل هي الأنسب لجدران الحماية؟ وسنركز على بيئتين شهيرتين هما بيئة " يونكس " (Unix) وبيئة النوافذ " وندوز إن تي " (Windows NT).

فبناء جدار الحماية يتطلب وجود خادم متصل بشبكة الإنترنت (خادم واحد على الأقل)، وحتى وقت قريب كان نظام التشغيل المعتاد هو نظام " يونكس " وكان هو الأكثر انتشارًا على خوادم شبكة الإنترنت. والآن دخلت بيئة " وندوز إن تي " حلبة السباق باعتبار أنها توفر نظام تشغيل متعدد المستفيدين يلائم احتياجات الأمن كما يلائم الشبكات. وبدأ هذا النوع في الانتشار مع جهود شركة " مايكروسوفت " وما بدأت توفره من تطبيقات أخرى تغري بالتوجه إلى هذه البيئة.

ومن المهم أن نعرف أنه ليس من الضروري أن يعمل جدار الحماية من خلال نفس نظام التشغيل الذي يشكل البيئة التي تستخدمها الشركة في أجهزتها وخوادمها. فمن

الممكن استخدام نظام التشغيل " يونكس " لجدران الحماية بينما تعتمد الشركة نظام " وندوز إن تي " كبيئة عمل لها [Ogletree ٢٠٠٠] وإنما يحكم اختيار جدار الحماية أساسًا الخصائص التي يتيحها لفرض السياسة الأمنية المطلوبة، وكذلك يحكم الاختيار إلى حد كبير خبرة المختصين الذين سيتولون تركيب جدار الحماية وتهيئته، فمن المهم أن يفهم هذا المختص إمكانيات نظام التشغيل الذي سيعمل جدار الحماية من خلاله، وأن يعرف نقاط الضعف فيه. فلابد أن يعرف مسئول الأمن مثلاً أنه من الممكن في نظام " يونكس " جعل ملف كلمات السر قابلاً للقراءة من الجميع (بدون حماية)، أو أن جدار الحماية نفسه يمكن الوصول إليه مباشرة من خلال شبكة الإنترنت وتغيير تهيئته.

نظام " لينكس" (Linux)أخذ في الانتشار هذه الأيام بسبب ميزته كأحد النظم المفتوحة (Open systems) ووقوف الكثير من الشركات المناوئة لشركة " ميكروسوفت " خلفه بالدعم والتأييد. ويتيح هذا النظام تسهيلات عديدة لمراقبة وقائع الاستخدام (Syslog)عن طريق مراقبة العديد من المنافذ، كما أنه يستطيع الاستفادة من البرامج الأخرى في النظام وما تخرجه من بيانات عن طبيعة الرسائل المارة في الشبكة.

نظام " وندوز إن تي " يمكن المستفيد من مراقبة عدد كبير من الوقائع وإن كان أسهل في الاستخدام لعدم الاستعانة ببرامج مساعدة كثيرة مثلما هو الحال مع نظام " يونكس ". وهذه السهولة في الاستخدام (لدرجة عدم الحاجة لمتخصص حقيقي) تعتبر ميزة كبيرة. وإن كان نظام " وندوز إن تي " أصعب في الاستخدام من ناحية أخرى بسبب صعوبة تهيئة جدار الحماية فيه، وذلك بسبب الطريقة التي يستخدم بها نظام " وندوز إن تي " بروتوكول (TCP/IP) لحديث عهدها به مقارنة بنظام " يونكس ". ولذلك فقد اضطرت شركة " مايكروسوفت " لإعادة بناء بروتوكول (TCP/IP) من الصفر ليناسب نظام " وندوز إن تي " مع ما اعترى هذه العملية من أخطاء، مما يعتبر نقطة ضعف أساسية في استخدام نظام " وندوز إن تي " [Zwicky ٢٠٠٠] ولكن هذه المشكلة لا تسبب خطورة كبيرة في حالة تصميم جدار الحماية بحيث يستخدم " موجهًا " يعمل بأسلوب تصفية الحزم، إذ يستطيع هذا الموجه أن يحقق الحماية المطلوبة

للأجهزة التي تستخدم " وندوز إن تي ".

في الحقيقة لا يخلو نظام تشغيل من النظم المتاحة " يونكس " و " لينكس " و" وندوز إن تي " من الثغرات الأمنية، وهذا ينطبق حتى على النسخ الحديثة من هذه النظم. وربما كان من العوامل الجديرة بالاعتبار وجود شركة قوية خلف منتج معين تستطيع مراقبة المشاكل ومتابعتها وحلها في وقت مناسب.

لذلك فإني أنصح مسئول الأمن عادة بأن يستخدم (كبيئة لجدار الحماية) نظام التشغيل الذي يعرف عنه الكثير ويتمكن من التعامل معه بكفاءة بغض النظر عن العوامل الأخرى.

٩-٤-٨ هل نشتري جدار حماية؟ أم نبنيه؟:

لا يجوز أن ننهي ما بدأناه في هذا القسم من مقارنة جدران الحماية دون أن نسأل أنفسنا السؤال الهام: هل نشتري جدار حماية جاهزًا؟ أم نقوم بمهمة البناء بأنفسنا؟

عند قيام جهة ما ببناء جدار الحماية الخاص بها سواء عن طريق موظفيها أو بالاستعانة بأحد المتخصصين فإنه بعد سنوات قليلة، وأحيانًا بعد شهور قليلة تطرح في الأسواق نظم أكثر تطورًا وذات إمكانيات أفضل! وربما كانت هذه النظم تناسب احتياجات المستفيد بشكل أفضل. ولكن على المستفيد أن يعرف احتياجاته على وجه الدقة حتى يستطيع اتخاذ القرار. وعلى الجهة التي تفاضل بين عملية الشراء والاتجاه إلى البناء أن تدرس جيدًا وضعها والموارد المتاحة لها سواء الموارد البشرية أو المالية، فالجهات التي لديها المال وليس لديها الخبراء يناسبها أكثر اختيار الشراء، بينما الجهة التي لديها المتخصصون ولديها الوقت الكافي لبناء النظام سوف تجد أن بناء النظام اختيار أفضل. وبالمتخصصين نعني ذوي الخبرة في عدة مجالات: في الإنترنت وفي

أمن المعلومات وفي برمجة نظم جدران الحماية وفي نظم التشغيل.

الجهات ذات الطابع الأمني المتميز مثل أجهزة المخابرات ووزارات الدفاع والداخلية تفضل بناء نظمها الدفاعية جميعها (ومن بينها جدران الحماية) بدلاً من شراء نظم جاهزة يعرف عنها العدو (وربما يعرف أكثر!).

وفي النهاية تعودت أن أنصح مسئولي أمن المعلومات بشراء النظم الجاهزة واستخدام المخارج الموجودة بها (Exits) لتنفيذ الكثير من التعديلات التي تحقق السياسة الأمنية للجهة. وأظن أن هذا الحل يتغلب على المشاكل التي يعرضنا لها قرار الشراء وقرار البناء معًا.

٩-٥ تصميم جدران الحماية (Firewall design):

تحدثنا في القسم الثاني من هذا الفصل (٩-٢ أنواع جدران الحماية) عن كيفية عمل الأنواع المختلفة من جدران الحماية. وسنتحدث في هذا القسم عن تصميم جدران الحماية، ونحن عادة لا نستخدم جهازًا واحدًا أو تقنية واحدة لتنفيذ جدار الحماية.

يجب عند تصميم جدار الحماية تحديد احتياجات الجهة بدقة حتى يمكن تحديد الدور المطلوب من جدار الحماية، وربما بعد استعراض البدائل المتاحة في الأسواق نضطر إلى إعادة تقييم الاحتياجات، ولكن من المهم أن تكون لدينا فكرة واضحة عما هو مطلوب من جدار الحماية. ومن المفهوم أن دور جدار الحماية هو تنفيذ السياسة الأمنية للموقع، أي أننا لابد أن يكون لدينا مسبقًا سياسة أمنية واضحة. ولقد تحدثنا عن هذه السياسة الأمنية في الفصل الرابع من هذا الكتاب. وتتضمن عملية تحديد الاحتياجات تحديد كل مما يلي:

٩-٥-١ الخدمات المطلوب تقديمها:

من المطلوب معرفة الخدمات التي يحتاج مستخدمو الموقع إلى طلبها من شبكة

الإنترنت، أو العكس بتقديم خدمات معينة من الموقع للعملاء عبر شبكة الإنترنت، إذا كان للمؤسسة موقع يزوره العملاء. وهل ستكون زيارة العملاء للموقع من خلال الإنترنت؟ أم أن العملاء سيسمح لهم بالدخول من بعد إلى شبكة المؤسسة الداخلية؟ كما يجب تحديد ما إذا كان للمؤسسة مؤسسات أخرى على علاقة معها، ومن ثم سيتم تبادل الخدمات مع هذه المؤسسات.

٩-٥-٢ مستوى الأمن المطلوب:

كثير من القرارات المطلوب اتخاذها خلال مرحلة تحديد الاحتياجات تتوقف على مستوى الأمن المطلوب. فهل المطلوب حماية بعض الأسرار النووية التي قد يؤدي انكشافها إلى تدمير العالم؟ أم أن كل المطلوب هو مجرد عدم كشف معلومات الشركة حتى لا يكون المدير في حرج؟ وهذا الحرج الذي يبدو بسيطًا قد يكون خطيرًا إذا كان سيكون أمام الرأي العام كله، أو على صدر الصفحات الأولى من الصحف. كثير من البنوك مثلاً ترى أن التشهير بها وبحدوث اختراق لها أكثر خطرًا من ضياع بضعة ملايين من الريالات، وقد شهد أحد البنوك في مدينة الرياض مؤخرًا حادث اختراق مؤلم بذل في محاولة كتمانه وإخفائه أكثر مما بذل في تأمين موقعه ضد الاختراق! وبصفة عامة، فمستوى الأمن المطلوب من جدار الحماية يجب تحديده في هذه المرحلة.

٩-٥-٣ حجم الاستخدام:

يجب معرفة أنواع خطوط الاتصال بشبكة الإنترنت، وعدد المستخدمين في الشبكة الداخلية، وعدد الزوار المتوقع للموقع، وما هي مدة بقاء كل زائر للموقع؟ وطبيعة استخدامه للموقع؟ ومدى حاجته للدخول إلى قواعد البيانات على الشبكةس الداخلية للمؤسسة؟

يؤثر حجم الاستخدام على تحديد سرعة وكفاءة الجهاز المستخدم كجدار حماية، أو ربما احتجنا لاستخدام أكثر من جهاز. كما يحدد احتياج الزائر للدخول إلى قواعد

٩ ـ ٥ ـ ٤ مدى خطورة انقطاع الخدمة:

من المهم تحديد مدى الأضرار التي قد تقع على المؤسسة إذا حدث انهيار لموقعها على شبكة الإنترنت، أو إذا حدث توقف للخدمة المقدمة إلى العملاء، أو الخدمة المقدمة إلى المستخدمين من الداخل إذا انقطع الاتصال بشبكة الإنترنت. وهل نتيجة ذلك ستكون مجرد مضايقة العملاء؟ أم أن ذلك سيسبب كارثة مثلما نتوقع عند انتشار استخدام تطبيقات التجارة الإلكترونية والحكومة الإلكترونية؟

٩ ـ ٥ ـ ٥ حجم الميزانية المتاحة:

يجب معرفة حجم الميزانية المخصصة لمشروع جدار الحماية ومجالات الإنفاق المتوقعة، كما يجب معرفة الاحتياجات المطلوبة من وقت الخبراء أو المستشارين. وربما كانت الميزانية المتاحة من أهم القيود التي تحكم كثيرًا من القرارات الخاصة بتصميم جدار الحماية أو اقتنائه.

٩ ـ ٥ ـ ٦ المتخصصون والخبراء المتاحون:

يجب معرفة عدد المتخصصين والخبراء الذين يمكن الاستفادة بهم في هذا المشروع ومدى خبرتهم في هذا المجال، فالبشر من أهم الموارد وأكثرها ندرة ويشكل العثور عليهم مشكلة، ويشكل الاحتفاظ بهم مشكلة أكبر. وكثيرًا ما يحدد هذا العامل كثيرًا من القرارات. فمثلاً إذا كان لدى المؤسسة عدد كبير من الموظفين ذوي الخبرة في نظام التشغيل " وندوز إن تي " ولم يكن لديها خبراء في نظام " يونكس "، فمن المنطقي أن تقرر المؤسسة الاتجاه إلى جدار الحماية المعتمد على " وندوز إن تي ". وإذا كان لدى المؤسسة شخص واحد سيكون مسئولاً عن جدران الحماية، فربما كان القرار الأفضل هو شراء جهاز حماية جاهز بدلاً من بناء هذا الجدار.

٩ـ٥ـ٧ بيئة التشغيل:

يجب تحديد أي قيود اجتماعية أو سياسية، مثل المقاطعة الاقتصادية لبعض الموردين أو تحبيذ للبعض الآخر. فعلى سبيل المثال نعلم أن بعض جدران الحماية تستخدم تقنيات التشفير، ونعلم أن هناك قيوداً على بيع وتصدير هذه التقنيات وانتقالها من دولة إلى أخرى. ولذلك فإذا كانت هناك حاجة إلى تركيب جدران حماية في فروع المؤسسة الموجودة في عدة دول، فيجب استخدام التقنيات التي لا يوجد عليها قيود.

٩ـ ٥ ـ٨ احتمالات تزايد حجم العمل في المستقبل:

لابد أن نأخذ في الاعتبار احتمالات تضاعف حجم المستفيدين وتضاعف حجم الإنترنت وانعكاس ذلك على جدار الحماية. هل جدار الحماية الذي نحن بصدد تصميمه سيظل مناسبًا بعد تضاعف حجم العمل؟ وهل زيادة إمكانيات جدار الحماية سهلة؟ أم سنضطر لتغييره بالكامل؟ فمع استخدام خادم البروكسي سيكون صعبًا إضافة خادم بروكسي آخر لأن ذلك يعني إعادة تهيئة أجهزة المستفيدين، وسيكون مستحيلاً (وليس صعبًا) إضافة مصفاة حزم أخرى، لأن فكرة مصفاة الحزمة تعتمد على مرور جميع الحزم بنفس المصفاة، وهذا سيحكم اختيار البديل المناسب.

٩ـ٦ تنفيذ جدران الحماية (Firewall implementation):

نقدم في هذا القسم الأخير من حديثنا عن جدران الحماية عدة أساليب لتنفيذ جدران الحماية حسب قرارات التصميم التي تحدثنا عنها في القسم السابق.

٩ـ٦ـ١ استخدام جهاز واحد (Single-box architecture):

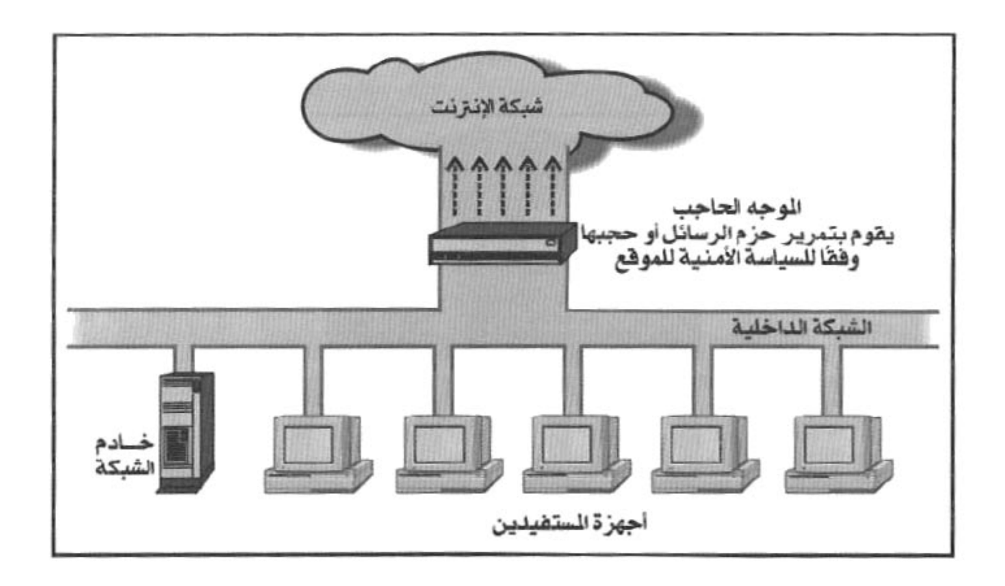
أبسط أساليب الاستخدام هي استخدام جهاز واحد (Single-box architecture)

يقع عند التقاء الشبكة الداخلية بشبكة الإنترنت. وهذا الجهاز إما أن يكون موجهًا حاجبًا (Screening router)، أو جهازًا مزدوج الاتصال (Dual-homed host)، أو أجهزة متعددة الاستخدام (Multiple-purpose boxes).

٩-٦-١-١ الموجه الحاجب (Screening router):

يبين الشكل (٩-٨) استخدام " الموجه الحاجب " (Screening router) عند مدخل الشبكة، ويصلح هذا الأسلوب إذا كان خادم الشبكة مؤمنًا بشكل جيد، وكان عدد البروتوكولات المستخدمة (الخدمات المقدمة من شبكة الإنترنت) محدوداً، وكذلك إذا كانت سرعة الاستجابة أهم بكثير من الأمن وهذا قد يحدث في بعض المواقع التي تؤدي خدمات عامة ومن المهم أن تؤدى الخدمة بسرعة ولا توجد معلومات يخشى من تسربها.

شكل (٩-٨)
استخدام الموجه الحاجب لتصفية حزم الرسائل

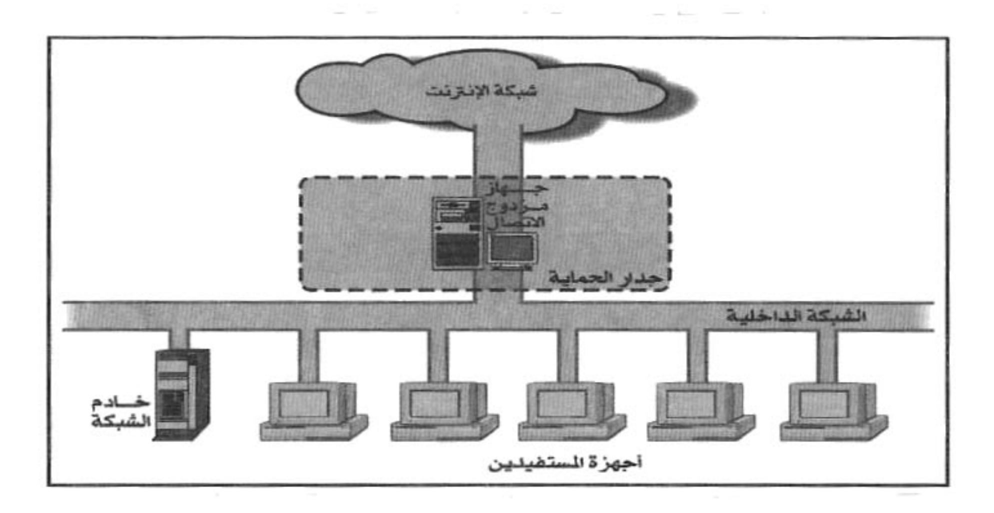


٩-٦-١-٢ الجهاز مزدوج الاتصال (Dual-homed host):

يبين شكل (٩-٩) استخدام الجهاز مزدوج الاتصال (Dual-homed host) كجدار حماية يفصل بين الشبكة الداخلية وشبكة الإنترنت. وهذا الجهاز يكون به أكثر من بطاقة شبكة، تتصل إحداها بالشبكة الداخلية والأخرى بشبكة الإنترنت، ويمكن أن يتصل بشبكات أخرى كذلك عن طريق بطاقات شبكة إضافية، ومن ثم فهو يستطيع توجيه حزم الرسائل إلى أي شبكة. ويصلح هذا الأسلوب عندما يكون حجم الرسائل المارة إلى شبكة الإنترنت من الشبكة أو الشبكات الداخلية محدوداً، وعندما لا تكون هذه الرسائل ذات حساسية عالية بالنسبة للمؤسسة، بمعنى أن أمنها لا يؤثر بشكل حاسم على أمن المؤسسة نفسها. ويستخدم هذا النوع كذلك إذا لم تكن المؤسسة تقدم خدماتها لعملائها عبر شبكة الإنترنت، أي لا يتم الدخول على شبكة المؤسسة وقواعد بياناتها من شبكة الإنترنت، وعندما تكون قواعد البيانات الموجودة في شبكة المؤسسة الداخلية لا تحتوي على بيانات حساسة أو خطيرة.

شكل (٩-٩)

استخدام الجهاز مزدوج الاتصال كجدار حماية

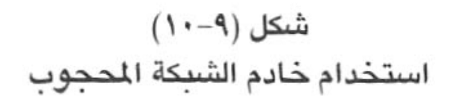


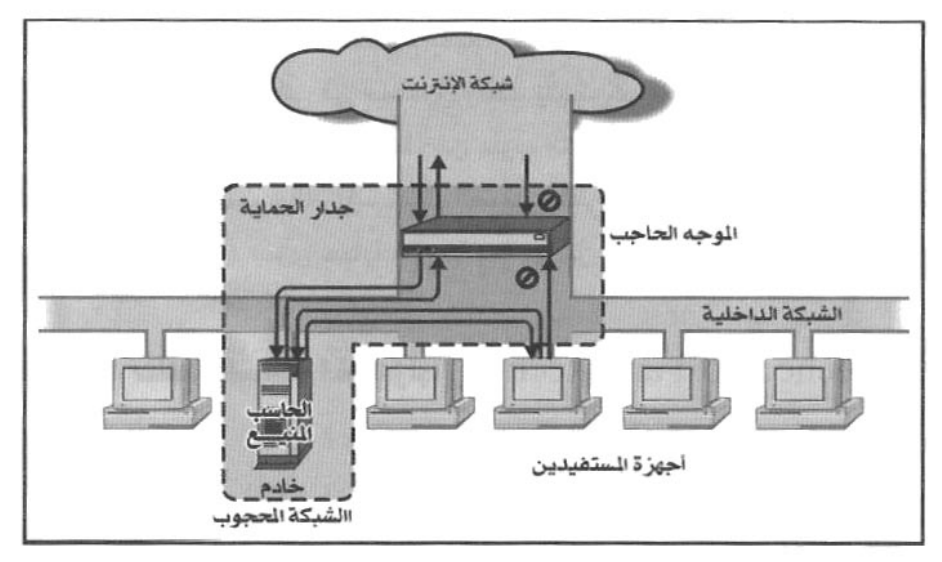
٩-٦-١-٢ الأجهزة متعددة الاستخدام (Multiple-purpose boxes):

يمكن استخدام بعض الأجهزة التي تقوم بأكثر من مهمة في نفس الوقت (Multiple-purpose boxes)، فتقوم بمهمة خادم البروكسي ومهمة مصفاة حزم الرسائل في آن معًا، وتأتي في صندوق واحد يتم تركيبه على حدود الشبكة وعند التقائها بالإنترنت. ومع ما لهذا النظام من عيوب التعارض بين مهمة البروكسي ومهمة المصفاة، إلا أنه يناسب حالة المؤسسات الصغيرة التي لا تقدم أي خدمة لعملائها عبر شبكة الإنترنت ولا تود سوى حماية الشبكة وما بها من أجهزة فقط.

٩-٦-٢ خادم الشبكة المحجوب (Screened host architecture):

أسلوب استخدام " خادم الشبكة المحجوب " (Screened host architecture) الذي يظهر في شكل (٩-١٠) هو الأسلوب الأكثر تطورًا من استخدام جهاز واحد لحماية الشبكة. ويقدم هذا النوع خدمات خادم الشبكة للمستفيدين، مع ربط خادم الشبكة بالشبكة الداخلية فقط وحجبه عن شبكة الإنترنت باستخدام " موجه حاجب " (Screening router) يتولى هذا الموجه مهمة تصفية الحزم المارة ومهمة حماية خادم الشبكة وهو الحاسب المنيع (Bastion host).

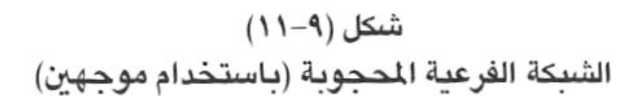

شكل (٩-١٠)
استخدام خادم الشبكة المحجوب



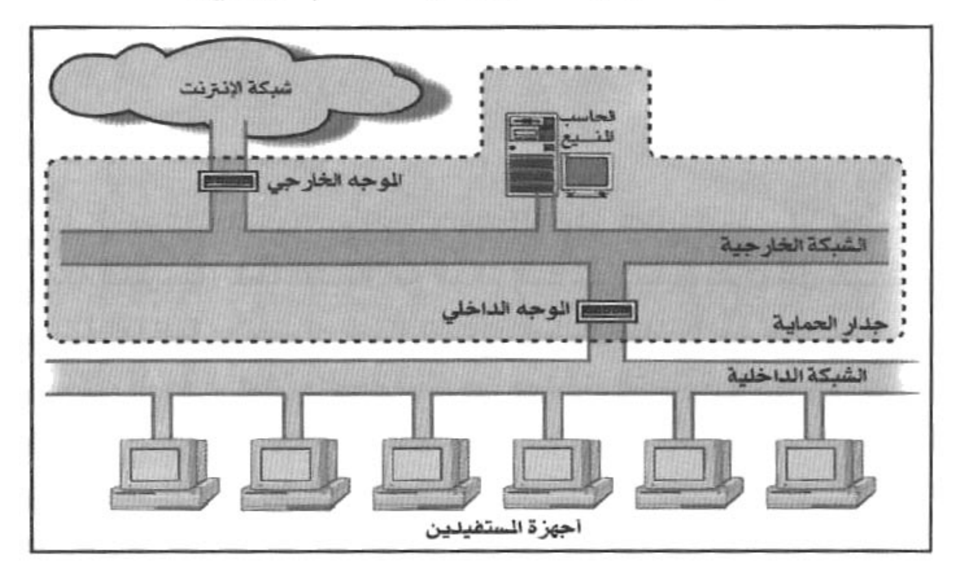
ويصلح هذا الأسلوب عندما يكون الدخول من شبكة الإنترنت محدوداً، وعندما يكون هناك تأمين إضافي للشبكة الداخلية علاوة على جدار الحماية (ولا يصلح هذا الأسلوب أبداً إذا كان خادم الشبكة المحجوب خادم إنترنت عاماً يؤمه الكثير من مرتادي شبكة الإنترنت، فهو لا يتحمل ضغط الدخول المتواصل).

٩-٦-٣ الشبكة الفرعية المحجوبة (Screened subnet architecture):

خطوة أخرى إلى الأمام في تشديد الحراسة هي استخدام " الشبكة الفرعية المحجوبة "(Screened subnet architecture)، ويضيف ذلك الأسلوب طبقة حماية أخرى إلى أسلوب " خادم الشبكة المحجوب "، وذلك بإضافة شبكة فرعية كاملة تتولى مهمة (عزل) الشبكة الداخلية عن الإنترنت. وبذلك نوفر الحماية لخادم الشبكة (الحاسب المنيع) كما يتبين من شكل (٩-١١).



شكل (٩-١١)
الشبكة الفرعية المحجوبة (باستخدام موجهين)



ويمتاز هذا التركيب عن أسلوب خادم الشبكة المحجوب بأننا قد حجبنا الحاسب المنيع (Bastion host) عن طريق عزله بواسطة الشبكة الخارجية، فإذا اخترقه المهاجم فإنه سيظل بعيدًا عن الشبكة الداخلية. ويصلح هذا التركيب لجميع الاستخدامات بلا تحفظ. في هذا الشكل (٩-١١) تظهر أربعة مكونات هي: " الشبكة الخارجية " (Perimeter network)، و" الحاسب المنيع "(Bastion host)، و" الموجه الداخلي " (Interior router)، و" الموجه الخارجي "(Exterior router)، وسنتحدث عن مهمة كل منهم بالتفصيل.

٩-٦-٣-١ الشبكة الخارجية:

تشكل الشبكة الخارجية (Perimeter network) طبقة الحماية الإضافية التي تحدثنا عنها في نهاية الفصل السابق عندما تحدثنا عن " الدفاع في العمق " وضرورة وجود أكثر من خط دفاع. فإذا حدث اختراق لهذه الشبكة فكل الرسائل التي سيطلع

عليها المهاجم هي الرسائل المتبادلة بين الحاسب المنيع وشبكة الإنترنت، أما الرسائل المتبادلة بين الأجهزة المرتبطة بالشبكة الداخلية وكذلك كل ما يدور في الشبكة الداخلية فسيظل في أمان بعيدًا عن أعين المتلصصين.

٩-٦-٣-٢ الحاسب المنيع:

يشكل هذا الحاسب المنيع (Bastion host) (وقد تتعدد الحاسبات المنيعة في الشبكة الخارجية) نقطة الاتصال مع العالم الخارجي، بحيث يتم تعامل مستخدمي الشبكة الداخلية مع خدمات شبكة الإنترنت (بشكل مباشر) عن طريق مرور حزم الرسائل بالموجه الداخلي والموجه الخارجي حيث تتم التصفية، كما سيتم استخدام الحاسب المنيع كخادم بروكسي، بحيث يتم تعامل مستخدمي الشبكة الداخلية مع خدمات شبكة الإنترنت (بشكل غير مباشر).

٩-٦-٣-٣ الموجه الداخلي:

مهمة الموجه الداخلي (Interior router) هي حماية الشبكة الداخلية من كل من شبكة الإنترنت ومن الشبكة الخارجية. وهو يتولى معظم مهام تصفية الحزم بفحص طلبات البيانات المرسلة إلى الإنترنت من مستخدمي الشبكة الداخلية. فإذا تمكن المهاجم من اختراق الحاسب المنيع فلن يستطيع الوصول إلى أجهزة الشبكة الداخلية والخدمات التي تقدمها وهي الهدف الذي يكون المهاجم عادة وراءه.

٩-٦-٣-٤ الموجه الخارجي:

مهمة الموجه الخارجي (Exterior router) هي حماية كل من الشبكة الخارجية والشبكة الداخلية من مخاطر الإنترنت. عادة يكون الموجه الخارجي موجودًا لدى مقدم الخدمة (Service provider)، ومن ثم يتولى مقدم الخدمة إدارته.

ويهتم الموجه الخارجي بتطبيق قواعد تصفية الحزم التي تحمي الأجهزة الموجودة بالشبكة الخارجية (أي الحاسب المنيع والموجه الداخلي). وتظهر أهميته بوجه خاص في حجب أي حزم قادمة من شبكة الإنترنت تحمل عنوان مصدر مزورًا. هذه الحزم التي تدعي ورودها من الشبكة الداخلية برغم أنها تكون آتية من مهاجم على شبكة الإنترنت. وحده الموجه الخارجي في موقعه هو الذي يستطيع كشف هذا التزوير.

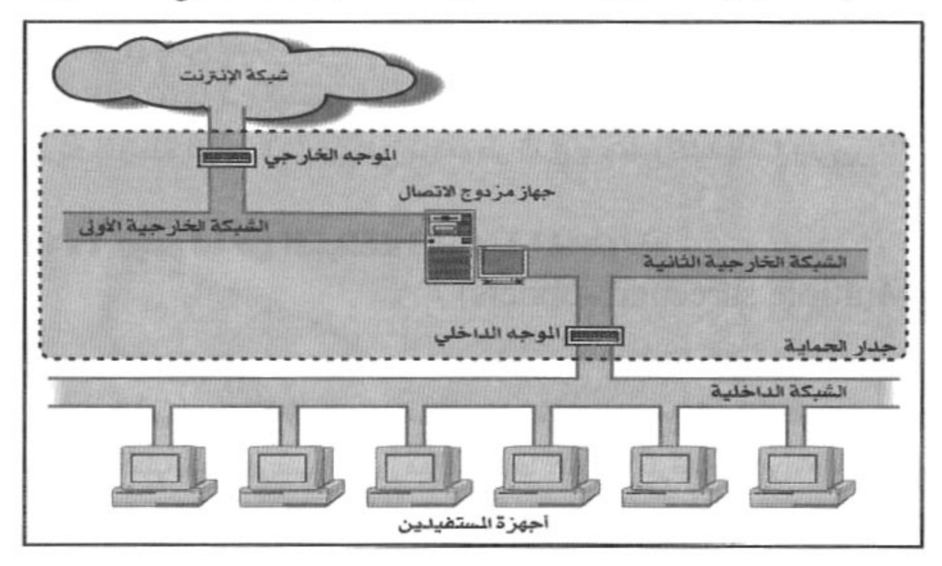
٩-٦-٤ مجموعة من الشبكات الفرعية المحجوبة (Multiple screened subnets):

بعض الشبكات لا تكتفي بوجود شبكة فرعية واحدة محجوبة وبالذات عندما تكون السياسة الأمنية معقدة وعندما تكون هناك قواعد كثيرة متعارضة وتكون الحاجة ماسة إلى تطبيقها جميعًا كما سنبين في استعراضنا لهذا التركيب. وفي هذه الحالة يتم استخدام " مجموعة من الشبكات الفرعية المحجوبة" (Multiple screened subnets).

٩-٦-٤-١ الشبكة الفرعية المحجوبة المقسمة (Split-screened subnet)

يبين شكل (٩-١٢) " الشبكة الفرعية المحجوبة المقسمة "(Split-screened subnet) حيث يوجد موجه داخلي وموجه خارجي، ولكن يفصل بينهما عدة شبكات. وتتصل هذه الشبكات (المحجوبة) ببعضها البعض عن طريق واحد أو أكثر من الأجهزة مزدوجة الاتصال (Dual-homed hosts) وليس عن طريق موجه. وتتبع بعض المواقع هذا الأسلوب للحصول على ميزة الدفاع في العمق الذي تحدثنا عنها من قبل، ولضمان حماية خادم البروكسي بواسطة الموجهات التي تكشف تزوير الحزم. كما تتم الحماية كذلك من خطر حدوث انهيار في النظام عندما يبدأ الجهاز مزدوج الاتصال بتوجيه الرسائل إلى جهات الاستقبال، فهذا الجهاز يستطيع أن يتحكم بشكل أكثر دقة من مصافي الحزم.

شكل (٩-١٢)
الشبكة الفرعية المحجوبة المقسمة (باستخدام جهاز مزدوج الاتصال)

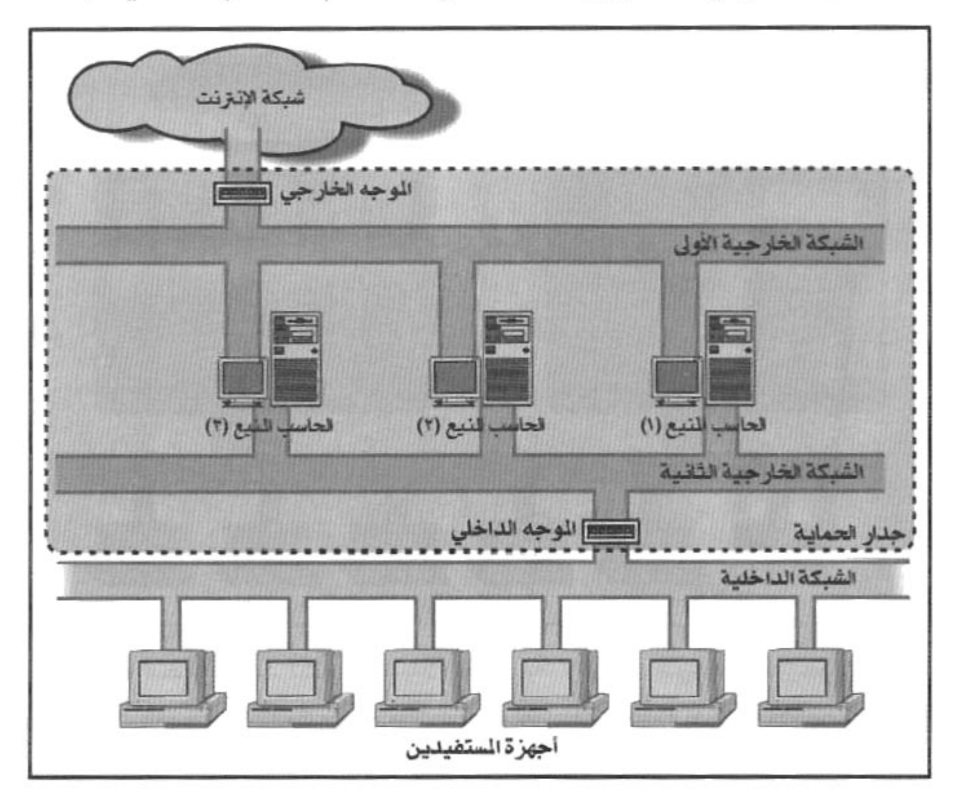


ويستخدم جدار الحماية من هذا النوع كذلك من جانب الجهات التي تقدم الخدمة لعملائها عبر شبكة الإنترنت وتخشى تعريض أجهزتها الداخلية وقواعد بياناتها الحساسة للخطر.

أما تلك الجهات التي تهتم بسرعة الأداء للأجهزة التي تستخدم الشبكة بكثافة فإنها تحاول منع استهلاك سعة الخطوط (Bandwidth) المخصصة لتقديم الخدمة للمستفيدين. هذه الجهات تدخل تعديلاً بسيطًا على التركيب المبين في شكل (٩-١٢) باستخدام الحاسبات المنيعة (Bastion hosts) بدلاً من الجهاز المزدوج الاتصال. ويبدو هذا التعديل في الشكل (٩-١٣).

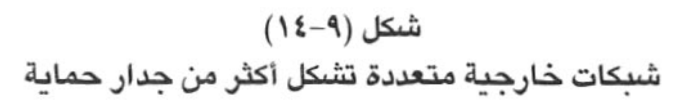
ويصلح هذا التركيب (الشبكة الفرعية المحجوبة المقسمة) للشبكات التي تحتاج إلى درجة أمن عالية، خاصة إذا كانت هذه الشبكة تقدم خدماتها للمستخدمين من خلال شبكة الإنترنت.

شكل (٩-١٣)
الشبكة الفرعية المحجوبة المقسمة (باستخدام الحاسبات المنيعة)



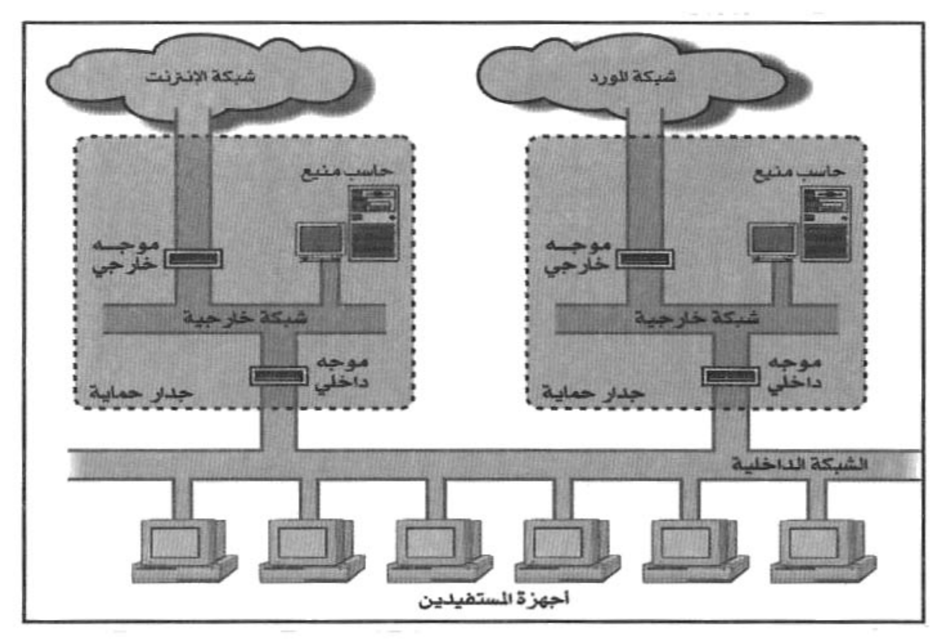
٩-٦-٤-٢ الشبكات الفرعية المحجوبة المستقلة
(Independent screened subnets)

قد تحتاج بعض الجهات إلى اقتناء أكثر من شبكة فرعية محجوبة مستقلة (Independent screened subnets)باستخدام موجهات خارجية منفصلة كما يبدو في الشكل (٩-١٤).



شكل (٩-١٤)

شبكات خارجية متعددة تشكل أكثر من جدار حماية

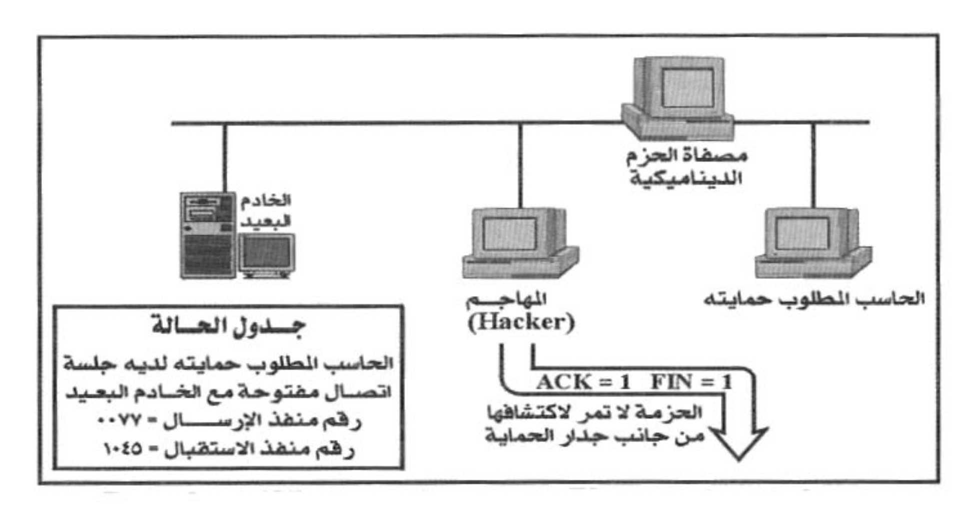


في هذه الحالة يوجـد أكثر من شبكة خـارجية، وبوجود مـوجهين خارجيين وشبكتين خـارجيتـين وموجهـين داخليين نـضمن عـدم وجود فـرصة لانقطاع الاتـصال بـشبكة الإنتـرنت. ومن المفهـوم أن هذا التـركيب سـيستخـدم اثنين من مقـدمي الخدمـة، وليس مقدم خدمة واحد، بحيث يكون لكل منهما اتصال منفصل بشبكة الإنترنت.

في هذه الحالة يجب مراقبة الموجهات بـشكل مكثف للتأكد من التزامها بتطبيق نفس السياسة الأمنية، وعند تعـديل السياسة الأمنية لأي منهمـا يجب تعديل السياسة الأمنية للموجهات الأخرى.

يبين الـشكل (٩-١٥) جـدار الحـماية الـذي يجب أن تـستخـدمه الـشركـات مقـدمة الخدمة، ويبدو في الشكل استخـدام أكثر من شبكة خارجيـة وأكثر من نقطة اتصال مع شـبكة الإنترنـت. ولا يجب أن تتساهل الجهـات مقدمة الخـدمة في تقديم جـدران حماية أقل من ذلك.

شكل (٩-١٥)
جدران حماية معقدة



هذا الأسلوب " الشبكات الفرعية المحجوبة المستقلة " يناسب الشبكات التي يهمها كثيرًا استمرارية الخدمة ولا تتحمل توقف اتصالها بشبكة الإنترنت ولو لفترة محدودة، كما يناسب الشبكات التي تحتاج إلى درجة أمن عالية، والتي ترتبط بشبكات أخرى منفصلة مثلما هو الحال مع الشركات مقدمة الخدمة.

في هذا الفصل، واستطرادًا لاستعراض تقنيات الحماية المختلفة، تحدثنا عن جدران الحماية وأنواعها، ومقارنة هذه الأنواع وكيفية الاختيار من بينها، كما تحدثنا عن أساليب تصميم جدران الحماية وتنفيذها سواء لدى الشركات أو لدى مقدمي الخدمة.

الفصل العاشر
الشبكات الخاصة الافتراضية

هذا هو الفصل الأخير من بين أربعة فصول تناولت تقنيات الحماية المستخدمة لتأمين شبكات المعلومات.

وهذا الفصل يعني بالشبكات الخاصة الافتراضية (VPN) فنبدأه بتوضيح مفهوم هذه الشبكة ومكوناتها وكيف يتم التخطيط لإنشائها. ثم نستعرض استخدامات هذه الشبكة وكيف يمكن أن تكون بديلاً عن مجموعة كاملة من أجهزة المودم، أو أن تكون بديلاً عن الشبكات الكبيرة الخاصة. ثم نوضح العيوب التي تكمن في الشبكات الخاصة الافتراضية.

في القسم الثالث من هذا الفصل نستعرض الأنواع المختلفة للشبكات الخاصة الافتراضية، ونقارن بين هذه الأنواع ليستطيع القارئ تحديد أي هذه الأنواع يناسب احتياجاته. ثم نبين الأساليب المختلفة لتنفيذ الشبكة الخاصة الافتراضية سواء باعتمادها على جدار الحماية، أو الموجهات، أو استخدام برمجيات خاصة. ونختم الفصل بكيفية اختبار الصلاحية الأمنية للشبكة.

١٠-١ مفهوم الشبكة الخاصة الافتراضية (VPN):

منذ ظهرت شبكة الإنترنت لم تظهر تقنية أخرى حملت معها كل هذه الآفاق الرحبة والإمكانيات غير المحدودة، وفي الوقت نفسه لم تظهر تقنية أخرى حملت معها كل هذه الأخطار والمخاوف والتحديات. ومع ازدياد تكلفة الشبكات الكبيرة Wide Area Net-) works)التي كان لزامًا على الشركات التي لها فروع بعيدة أن تنشأها، مع ازدياد هذه التكلفة وانتشار استخدام شبكة الإنترنت وسهولة الاتصال بها جاءت فكرة الشبكة الخاصة الافتراضية (VPN) ولكنها جاءت ومعها من المخاوف ما كان كافيًا لوأدها في المهد لولا تقدم تقنيات أمن وحماية المعلومات وعلى رأسها تقنيات التشفير (Encryption)، وتقنيات التحقق من الشخصية (Authentication) والآن وبعد انقضاء عامين على بداية الألفية الميلادية الثالثة نجد العديد من الشركات التجارية

والمالية والجامعات وبعض الوزارات والإدارات الحكومية تقيم شبكاتها الخاصة الافتراضية. وبدأت البنوك التي أرادت دخول عصر البنك الإلكتروني(e-banking) وبنوك الإنترنت (I-banking) في إنشاء شبكاتها الخاصة الافتراضية.

١٠-١-١ مكونات الشبكة:

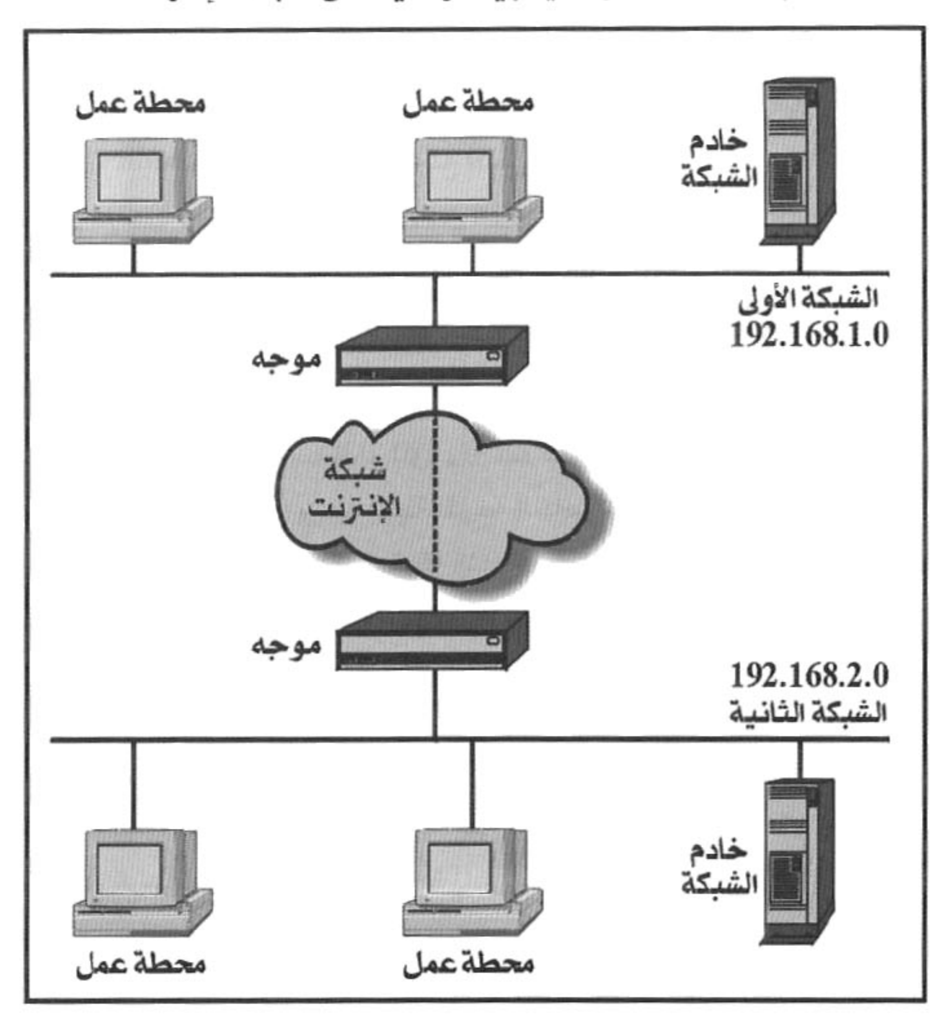
يمكن تعريف الشبكة الخاصة الافتراضية (VPN) أو (Virtual Private Net-works) بأنها قناة اتصال مشفرة ومأمونة تتم من خلال شبكة عامة غير مأمونة مثل شبكة الإنترنت العالمية.

ولما كانت شبكة الإنترنت غير مأمونة فقد كان من الضروري اللجوء إلى التشفير (Encryption) وإلى أساليب التحقق من شخصية المرسل (Authentication) لحماية البيانات خلال مرورها. وتتعامل الشبكة الخاصة (VPN) مع البيانات بصرف النظر عن نوع الخدمة المطلوبة (Service independent)، أي أن كل المعلومات المتبادلة بين أطراف الشبكة يتم نقلها من خلال قناة التشفير سواء كانت هذه المعلومات تنقل من خلال خدمة نقل الملفات (FTP)، أو البريد الإلكتروني (SMTP)، أو صفحات النسيج (Web)، أو غيرها من الخدمات التي تحدثنا عنها في الفصل الثالث.

يبين الشكل (١٠-١) مثالاً شائعًا لتركيب الشبكة الخاصة الافتراضية. يظهر الشكل شبكتين مستقلتين تتصل كل منهما بشبكة الإنترنت، وتحتاج هاتان الشبكتان إلى تبادل المعلومات فيما بينهما بطريقة آمنة، لأن بعض هذه المعلومات له صفة السرية. ولكي نحمي هذه المعلومات يتم إنشاء شبكة خاصة افتراضية (VPN) بين هذين الموقعين.

شكل (١٠-١)

شبكة خاصة افتراضية بين موقعين على شبكة الإنترنت



١٠-١-٢ التخطيط لإنشاء الشبكة:

يتطلب إنشاء الشبكات الخاصة الافتراضية بعض التخطيط المسبق، فيجب أن تقوم الشبكتان المشاركتان بالخطوات التالية:

- يجب أن يوفر كل موقع جهازًا في مدخل الشبكة يسمح بالتعامل مع شبكة (VPN) أي (VPN-cabable)، ويمكن أن يكون هذا الجهاز موجهًا (Router)، أو جدار حماية (Firewall)، أو جهازًا مخصصًا لغرض الاتصال بشبكة (VPN)
- يجب أن يعلم كل موقع، على سبيل الحصر، عناوين الشبكة الفرعية (IP subnet IP addresses)المستخدمة بواسطة الموقع الآخر.
- يجب أن يتفق كلا الموقعين على أسلوب التحقق من الشخصية (Authentication) وأسلوب تبادل شهادات التعريف الرقمية (Digital certificates)
- يجب أن يتفق كلا الموقعين على أسلوب التشفير، وأسلوب تبادل مفاتيح التشفير عند الحاجة لذلك.

ويبين الشكل (١٠-١) استخدام الموجهات عند مداخل الشبكتين المشتركتين، أي عند مداخل نفق شبكة (VPN) ويجب تهيئة الموجه الخاص بالشبكة الأولى بحيث تكون كل الرسائل المارة به والمتجهة إلى الشبكة الثانية (١٩٢,١٦٨,٢,٠) مشفرة باستخدام نظام (DES) للتشفير مثلاً، ويسمى ذلك " نطاق التشفير " (Encryption domain) ويجب أن يعرف الموجه الخاص بالشبكة الأولى أن أي معلومات يتم استقبالها من الموجه الخاص بالشبكة الثانية تحتاج إلى فك شفرتها (Decryption) قبل تسليمها للمستفيد النهائي. كما يجب تهيئة الموجه الخاص بالشبكة الثانية بنفس الأسلوب، أي كي يقوم بتشفير كل الرسائل الموجهة إلى الشبكة الأولى (١٩٢,١٦٨,١,٠) ويفك شفرة كل الرسائل المستقبلة من الموجه الخاص بالشبكة الأولى.

أما الرسائل التي يتم إرسالها إلى أي جهة أخرى في شبكة الإنترنت فإنها تنقل دون تشفير. فقط الاتصالات التي تتم بين هاتين الشبكتين هي التي يتم تشفيرها، وهذا ما ذكرنا أنه يسمى " نطاق التشفير " (Encryption domain) فإذا كانت هناك حاجة لإنشاء عدة شبكات خاصة (VPNs) فيجب تعريف نطاقات تشفير متعددة.

١٠ ـ ١ ـ ٣ جهاز تحليل الشبكة:

في بعض الشبكات الخاصة الافتراضية يوضع جهاز تحليل شبكة (Network analyzer) بين الموجهين بحيث يعيد إرسال كل حزم الرسائل مستخدماً عنوان إرسال وعنوان استقبال مختلفين، فأنت لا ترى عنوان المرسل إليه الحقيقي، أو عنوان مرسل الرسالة الحقيقي (Source or Destination host IP address)، إذ إن هذه المعلومات يتم تشفيرها مع بيانات الرسالة نفسها، وبعد تشفير حزمة الرسالة الأصلية يضع الموجه المعلومات المشفرة (النص والعنوان المشفرين) ضمن حزمة جديدة لها مقدمة جديدة تستخدم عنوان الموجه كعنوان المصدر وتضع عنوان الموجه في الطرف الآخر كعنوان المرسل إليه، وهذا ما يطلق عليه أسلوب " النفق "(Tunneling)، وهو ما يضمن أن المهاجم المتلصص لن يكون في مقدوره معرفة أي الرسائل المارة في الشبكة هي التي تستحق عناء المهاجمة وكسر الشفرة، إذ إن كل حزم الرسائل تستخدم عناوين الموجهات وليس عناوين المرسل الحقيقي أو المستقبل الحقيقي.

بوجود " نفق افتراضي " يمر بين كل من الموجهين، فإن المؤسسة التي تستخدم الشبكة الافتراضية يصبح لها مجال عنونة خاص خلال شبكة الإنترنت، فيستطيع أحد الأجهزة في الشبكة الأولى أن يرسل رسالة إلى جهاز آخر ضمن الشبكة الثانية دون الحاجة إلى ترجمة عنوان الشبكة الخاص بالجهاز المرسل إليه، ذلك لأن الموجه قد أودع معلومات مقدمة الرسالة كبيانات ضمن الرسالة المرسلة عبر النفق (فالنفق، ككل نفق، له مخرج واحد فقط). وعندما يتلقى الموجه الخاص بالشبكة الثانية حزمة البيانات فإنه ببساطة ينزع الغلاف الخارجي للرسالة ثم يفك شفرة الرسالة الأصلية، وعندئذ يقوم بتوصيل البيانات إلى المستقبل الحقيقي في شبكته. هناك ميزة أخرى لا يجب أن نغفل عنها عند استخدام هذا النوع من الشبكات، ألا وهي أن أجهزة المستخدمين لا تحتاج أن تستخدم برمجيات تشفير أو أن تنشغل بعمليات التشفير وفك الشفرة، فكل هذا يتم آلياً عند مرور البيانات بين الموجهين.

١٠ـ٢ استخدامات الشبكة الخاصة الافتراضية:

يمكن أن تحل الشبكة الخاصة الافتراضية محل قائمة كاملة من التقنيات والأجهزة والكابلات، ولا أجد لها عيوبًا سوى الجهد المطلوب لتهيئة أجهزتها مثل الموجهات وغيرها. وأعتقد أنه بتقدم التكنولوجيا فربما نرى هذه العمليات قد أصبحت تتم بجهد أقل وبقدر أكبر من الآلية. فيمكن مثلاً إتمام عملية التعارف بين الموجهات آليًا، وتبادل مفاتيح التشفير آليًا، وذلك قبل عملية تبادل الرسائل، وبمجرد الانتهاء من الإرسال والاستقبال يتم إغلاق الشبكة آليًا إلى حين الحاجة إلى تبادل الرسائل من جديد.

صحيح أن استخدام هذا النوع من الشبكات آخذ في التزايد والانتشار، إلا أننا نستطيع أن نحدد مجالين أساسيين لاستخدامها هما:

- أن تكون بديلاً عن مجموعة كاملة من أجهزة المودم.
- أن تكون بديلاً عن الشبكات الكبيرة الخاصة (Dedicated WANs).

١٠ـ٢ـ١ الشبكة الخاصة الافتراضية كبديل عن أجهزة المودم:

إذا قمت بزيارة أي مركز حاسب آلي في وزارة أو شركة كبيرة لها فروع متعددة، فلابد أنك ستلاحظ مجموعة من الكبائن التي تحتوي على العديد من أجهزة المودم التي تصل المركز الرئيسي بالفروع. هذه الغابة من أجهزة المودم تشكل همًا حقيقيًا لمدير الشبكة؛ ففضلاً عن تكلفتها الباهظة التي لا تحتملها ميزانيات الشركاست المتوسطة أو الصغيرة نجد أن معظمها يعاني من سوء التهيئة أو الحاجة إلى إعادة التهيئة من آن لآخر.

لذلك فإن البديل كان (الشبكة الخاصة الافتراضية) التي جاءت لتربط مثل هذه الجهة بفروعها البعيدة، وتقلص إلى حد كبير من التكلفة والجهد والعناء، فلن يعود هناك هذا العدد الكبير من خطوط الهاتف أو من الأرقام التي تبدأ بالرقم (٨٠٠) لتتيح لموظفيها إمكانية الاتصال المجاني عن بعد بشبكة المعلومات الخاصة بالشركة. ويعفي هذا الحل من الحاجة إلى تطوير خطوط الهاتف لكي تدعم التقنيات الجديدة مثل تقنية (ISDN) عند إدخالها، وإنما سيتم كل شيء من خلال شبكة الإنترنت.

ولكن قرار إنشاء الشبكة (VPN) وإتاحتها لاستخدام عملاء المؤسسة أو موظفيها عن بعد لابد وأن يخضع لاعتبارات أخرى، فكما يقول الإنجليز: (There is no free lunch) أي أن كل شيء بثمنه، فلهذا الأسلوب بعض العيوب وهي أن أمن المستفيدين عن بعد قد يتأثر عند استخدامهم للشبكة؛ ففي وجود بعض أدوات الاختراق والتلصص المتاحة مجاناً على شبكة الإنترنت، وسهولة الحصول عليها، مثل(L•ph's Netcat) أو (Cult of the Dead Cow's Back Orifice). في ظل وجود هذه الأدوات وسهولة استخدامها، فإن أمن المستفيدين الذين يستخدمون الشبكة عن بعد يصبح في خطر شديد. ونلاحظ أن معظم الشركات التي تقدم خدمة الإنترنت(ISPs) لاتقدم لهذا النوع من المستفيدين عن بعد أي جدار حماية (Firewall)، مما يعني أن الأجهزة التي تتصل عن بعد مفتوحة تماماً أمام أي هجوم. والأمر الأكثر خطورة هو أن المهاجم في حالة نجاحه في اختراق أحد الأجهزة التي تتصل عن بعد فسيكون في استطاعته أن يستخدم " نفق الشبكة " (VPN tunnel) لمهاجمة الشبكة الداخلية نفسها عن طريق هذه الثغرة المتمثلة في المستخدم عن بعد. أي أن السماح باستخدام (VPN) عن بعد في هذه الحالة يعني إضافة ثغرة أخرى في جدار الحماية الخاص بالشبكة الداخلية، وكلما زادت الثغرات زادت فرصة المهاجمين في اختراق الشبكة.

بصفة عامة، يجب قبل اتخاذ قرار السماح للمستخدمين عن بعد بالدخول إلى الشبكة أن نجيب عن الأسئلة التالية:

[١] كم سيكون عدد المستخدمين الذين سيستخدمون الشبكة في نفس الوقت (Concurrent users)؟ فكلما زاد عددهم زادت الحاجة إلى طاقة استيعاب أكبر للشبكة.

[٢] ما هي الأوقات التي سوف يتصل خلالها هؤلاء المستخدمون عن بعد بالشبكة؟ فإذا كانت هذه الأوقات هي أوقات العمل الرسمية، فستكون هناك حاجة إلى خطوط اتصال أسرع بمقدم الخدمة وكذلك إلى أجهزة أسرع (خادم أسرع، موجه أسرع، جدار حماية أسرع...).

[٣] ما هي الخدمات التي سيحصل عليها المستخدمون عن بعد من خلال شبكة (VPN)؟ فإذا كانت هذه الخدمات من النوع الذي يحتاج سعة أكبر للخطوط (Bandwidth-intensive applications) مثل التشارك في الملفات، فلابد من الحصول على خطوط اتصال أسرع بالإنترنت، وعلى أجهزة أسرع كما أسلفنا.

[٤] ما هو نوع التشفير الذي تخطط المؤسسة لاستخدامه؟ إذا كان هناك اتجاه لاستخدام وسائل تشفير ذات مفتاح طويل (Large key algorithm) مثل خوارزمية " التشفير الرقمي الثلاثي " (Triple DES) مثلاً، فلابد من توفير أجهزة تشفير أسرع.

١٠-٢-٢ الشبكة الخاصة الافتراضية كبديل عن الشبكات الكبيرة:

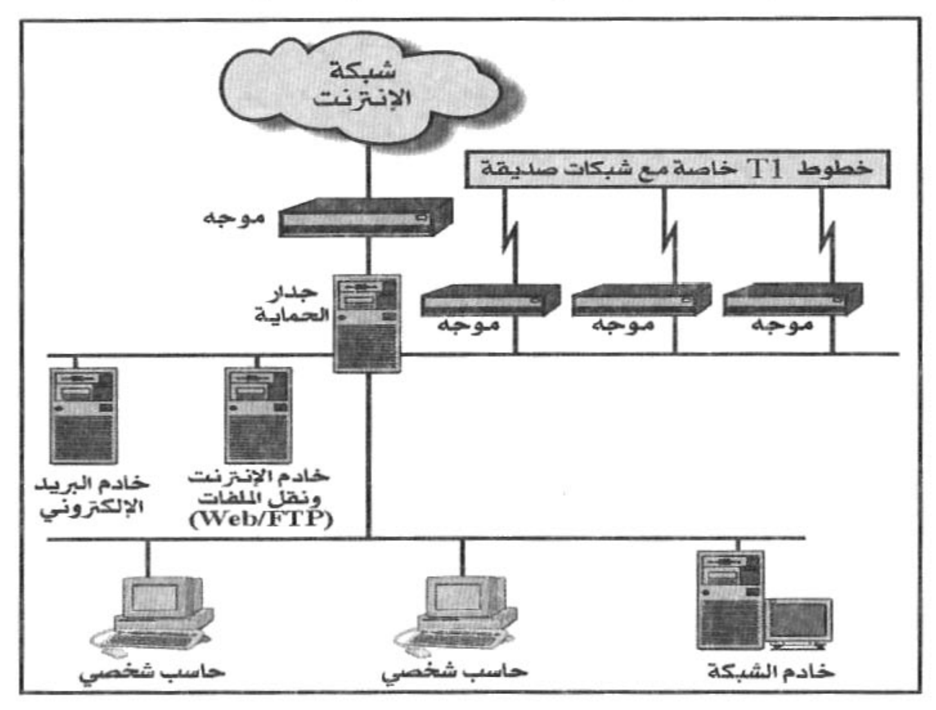
من المفهوم أن الشبكات الخاصة الافتراضية تصل بين شبكتين متباعدتين جغرافيًا عن طريق شبكة الإنترنت. وتصبح الفائدة أعظم إذا كان الموقعان بعيدين جدًا، كأن يكون الربط بين مقر الشركة في الرياض وفرع الشركة في الولايات المتحدة مثلاً، فبدلاً من دفع تكلفة دائرة هاتفية تحيط بنصف الكرة الأرضية، فإن كل فرع عليه أن يدفع تكلفة اتصاله بمقدم الخدمة المحلي فقط. وفي هذه الحالة تصبح شبكة الإنترنت هي العمود الفقري (Backbone)الذي يربط هاتين الشبكتين.

وحتى في حالة تقارب الموقعين تظل لشبكة (VPN) مزايا الاتصال دون الحاجة إلى خطوط خاصة مستأجرة (Leased lines)، فإنشاء نفق الشبكة (VPN tunnel) سهل ومرن، أي يمكن تعديله في أي وقت.

ويبين الشكل (١٠-٢) شبكة داخلية يحميها جدار حماية (Firewall) كما يوجد في جزء من الشبكة خادم الإنترنت (Web server) ومحول البريد الإلكتروني (SMTP relay). كما توجد في جدار الحماية بطاقة شبكة (Network card) إضافية لتوفير الحماية لعدد من خطوط (T١) الخاصة. هذه الخطوط مهمتها

توصيل الشبكة بعدة شبكات صديقة، ومن ثم يتم من خلالها تبادل المعلومات الحساسة غير المرغوب في مرورها عبر الإنترنت. هذه المعلومات الحساسة يمكن نقلها بواسطة البريد الإلكتروني أو بروتوكولات نقل الملفات (FTP).

شكل (١٠-٢)
شبكة تستخدم خطوطًا خاصة لحماية المعلومات الحساسة



سوف يواجه النظام المبين في الشكل (١٠-٢) عدة مشكلات، ربما كان أهمها " التوجيه "، إذ إن جدار الحماية قد يحتاج إلى أن تتم برمجته بحيث يتم تسجيل المعلومات التي يحتاج إليها لتوجيه الرسائل لكل من الشبكات البعيدة (الصديقة)، وإلا فإن جدار الحماية سيرسل الرسائل الموجهة لهذه الشبكات عن طريق الإنترنت، وهو التوجيه الافتراضي (Default) وفي حالة حدوث أي تغيير في عنوان إحدى هذه الشبكات يلزم

إعادة تهيئة جدار الحماية. وكثير من البدائل التي يمكن أن تحل هذه المشكلة تتطلب وجود أجهزة مماثلة أو تهيئة مماثلة لدى الشبكات البعيدة، وهو أمر من الصعب توقعه. وتتفاقم المشكلة إذا كانت إحدى الشبكات البعيدة تستخدم مجال عنونة افتراضي، أي أنها تعطي عنوان شبكة (IP address) غير حقيقي. في هذه الحالة هناك حاجة إلى المزيد من البرمجة والمزيد من الجداول المطلوب معالجتها [Brenton ١٩٩٩].

ثم نأتي إلى النقطة الأخطر طالما أن موضوعنا دائمًا هو أمن شبكات المعلومات.. ماذا لو تواجد أحد المهاجمين في إحدى هذه الشبكات البعيدة وقام هذا المهاجم بشن هجوم على شبكة بعيدة أخرى من الشبكات الصديقة؟ هذا التكوين الذي أوضحناه في الشكل (١٠-٢) يتيح فرصة مثالية لهذا المهاجم لكي يهاجم مؤسسة أخرى من خلال مؤسستنا دون أن ندري.

يكمن حل كل هذه المشاكل في وضع شبكة خاصة افتراضية (VPN) محل هذه الخطوط الخاصة، وإدارة عدة شبكات خاصة (VPNs) سيكون أسهل بكثير وأرخص بكثير من التعامل مع الدوائر الهاتفية الخاصة.

١٠-٢-٣ عيوب الشبكات الخاصة الافتراضية:

برغم أن الشبكات الخاصة الافتراضية (VPNs)، كما بينا، لها العديد من المزايا الاقتصادية والأمنية التي تتفوق فيها على استخدام الخطوط الخاصة للاتصال عن بعد، إلا أن هناك بعض العيوب التي يجب ألا نغفل عنها:

[١] بسبب طبيعة شبكة الإنترنت العالمية حيث يتم توجيه حزمة البيانات (IP pa-cket) من خلال خطوط اتصال متعددة قد يكون بعضها سريعًا وبعضها الآخر بطيئًا، فإن سرعة الإرسال في شبكة (VPN) تكون رهنًا بأبطأ خطوط الاتصال التي تمر بها حزم الرسائل مما يعطل الاتصال ويجعله محدودًا بأبطأ هذه الخطوط [Ogletree ٢٠٠٠].

[٢] عندما نستخدم الخطوط الخاصة، فإننا نتحكم تماماً في الأجهزة التي لدينا أو التي لدى الفروع الأخرى، بل إنك تستطيع توقيع عقد يضمن استجابة سريعة ومستوى معيناً من الخدمة ، أما في حالة شبكة الإنترنت فإننا لا نستطيع التحكم في الأجهزة التي تقوم بنقل معلوماتنا من مكان إلى أخر على الشبكة. فإذا حدث عطل في أي نقطة عبر خط الاتصال فإن هذا العطل قد يسبب تأخيراً في وصول الرسائل أو ربما تعطلاً كاملاً للشبكة، وأنت بالطبع لا تستطيع توقيع عقود ضمان مستوى الخدمة عبر الإنترنت!

[٣] إذا كان المستخدمون عن بعد في شبكتك يتعاملون مع الشركات المحلية لتقديم خدمة الإنترنت (Local ISPs)بأسلوب الاتصال المراقم (Dial-up access)، فيجب أن نختبر نوعية الخدمة التي تقدمها هذه الشركات، فإذا كان المستخدم عن بعد لا يستطيع الدخول إلى الشبكة خلال ساعات العمل أو في الوقت الذي يحتاج فيه إلى الدخول إلى الشبكة ـ بسبب انشغال خطوط مقدم الخدمة ـ فإن الاتصال من خلال المودم قد يكون أفضل.

[٤] في حالة وجود عدد محدود من المستخدمين عن بعد فإن الشبكة الخاصة الافتراضية تعتبر حلاً جيداً اقتصادياً وأمنياً، أما إذا كان عدد المستخدمين عن بعد كبيراً فربما كانت العودة إلى " غابة أجهزة المودم " أقل تكلفة من دفع التكلفة اللازمة لاتصال كل من هؤلاء المستخدمين عن بعد بمقدم الخدمة.

١٠ ـ ٣ أنواع الشبكات الخاصة الافتراضية ومقارنتها:

يخضع اختيارنا للشبكة الخاصة الافتراضية لعدة عوامل مثل التكلفة، والمرونة، ودرجة التحكم في السياسة الأمنية [Erbschloe ٢٠٠١].

فيما يخص التكلفة، تفضل كثير من الجهات البدء بشبكة بسيطة، ثم تبدأ في الإضافة إليها شيئاً فشيئاً ، وبذلك يمكن تقليل النفقات في البداية.

أما المرونة فربما كان أول المتأثرين بها هم المستخدمون عن بعد والذين قد يدخلون

إلى شبكة المؤسسة من أماكن متعددة وباستخدام وسائل تكنولوجية مختلفة (باستخدام هاتف ثابت أو متحرك، ومن خلال مقدم خدمة عام أو مقدم خدمة خاص لديه جدار حماية. . وهكذا). فالمستخدم المتنقل (Mobile user)يحتاج إلى خاصية " التجوال " (Roaming)، ولذلك لابد أن تتمتع شبكة (VPN)المختارة بهذه القدرة. كما تعني المرونة القدرة على النمو مع نمو احتياجات المؤسسة المستفيدة.

أما التحكم في السياسة الأمنية فهو يعني الكثير بدءًا من مستوى التشفير وآلية التحقق من الشخصية، إلى القدرة على المراقبة وتسجيل العمليات التي تتم من جانب المستخدمين (خاصة المستخدمين عن بعد). ويعني ازدياد القدرة على التحكم في السياسة الأمنية المزيد من المرونة، ولكنه في نفس الوقت يعني المزيد من التكلفة. وتجنح معظم الشركات إلى الحصول على درجة أكبر من التحكم في السياسة الأمنية حتى لا تترك هذه الأمور بيد مزود الخدمة. ونحن نعلم أن الكثير من مزودي الخدمة في المملكة يفتقرون إلى تنفيذ سياسات أمنية محكمة، فقد حدث أن تم العديد من الاختراقات لأجهزة بعض مزودي الخدمة، وكانت النتيجة أن بعض الجهات في مدينة الرياض تعرضت للاختراق بسبب ضعف السياسة الأمنية المقدمة من الشركة مقدمة الخدمة التي تتبعها هذه الجهات.

ولكي نتحدث عن أنوا ع الشبكات نجد أن هناك عديدًا من الأنواع تتراوح بين أقصى اليمين حيث نجد شبكات (VPN) تقوم بتركيبها وصيانتها الشركة أو المؤسسة بنفسها، وفي هذه الحالة لا يتعدى دور مقدم الخدمة (ISP) مجرد التوصيل بشبكة الإنترنت. وفي أقصى اليسار نجد الشبكة التي يترك تركيبها وصيانتها بالكامل لمقدم الخدمة ولا يكون للشركة أو المؤسسة دور يذكر في التحكم في الشبكة.

١٠-٣-١ الشبكة التي تديرها المؤسسة:

هذا النوع من الشبكات (Self-Deployed VPN) الذي تتولى المؤسسة تركيبه وإدارته بالكامل، يتم تركيبه في مقر المؤسسة ويرتبط بكل جهاز حاسب يتصل بمقر

المؤسسة عن بعد. والميزة الأساسية في هذا النوع هي " المرونة "، فلا تهم وسيلة الاتصال التي يستخدمها المتصلون عن بعد سواء كانت وسيلة لاسلكية أو الهاتف أو عن طريق مقدم خدمة محلي، وفي جميع الأحوال ستوفر شبكة (VPN) نفس المستوى من الخصوصية. هذا بالإضافة إلى ميزة التحكم الكامل للمؤسسة في شبكتها وفي سياستها الأمنية.

أما عيوب التحكم الكامل في شبكة (VPN) فهو العبء الكبير الملقى على عاتق مسئول أمن المعلومات ومسئول الشبكة، لذلك نجد أن كثيرًا من موردي (VPN) يقدمون تسهيلات إضافية تساعد في تنفيذ إجراءات التحكم في السياسة الأمنية. وباختصار شديد فهذا النوع يصلح أكثر للشركات الكبيرة ذات الفروع المتعددة [Erbschloe ٢٠٠١].

١٠-٣-٢ الشبكة التي يديرها مقدم الخدمة:

هذا النوع من الشبكات (ISP VPN Solution) أصبح واسع الانتشار في الوقت الراهن، وبالذات في المملكة العربية السعودية، حيث يتولى خبراء أمن المعلومات لدى مقدمي الخدمة طمأنة الشركات المستفيدة والبنوك المستفيدة على أمن معلوماتهم واتصالاتهم. وتعتبر هذه الخدمة من الخدمات الهائلة التي يقدمها مقدمو الخدمة، بشرط أن يؤدوها بشكل سليم!!.

قد تسند المؤسسات المستفيدة بعض الخدمات فقط، وليس كلها، لمقدم الخدمة؛ فتحتفظ مثلاً بجزئية التحقق من شخصية المتصل (Authentication) ولذلك يعرض مقدمو الخدمة مستويات مختلفة من خدمة (VPN) مما يسمح بخفض التكلفة على المؤسسات المستفيدة. ولعل هذه هي الميزة الرئيسية لهذا النوع؛ ففي هذا النوع تتفادى المؤسسات تعيين وتدريب متخصصين يتولون مهمة تركيب وإدارة هذه النظم. هناك أيضاً ميزة البساطة؛ ففي كثير من هذه الأنواع لا تكون هناك حاجة لتركيب برمجيات معينة لدى العملاء المتصلين عن بعد. تستطيع المؤسسات المستفيدة كذلك في ظل هذا

النوع من شبكات (VPN) أن تظل تستخدم " غابة أجهزة المودم " التي لديها وتنتقل بشكل تدريجي إلى الشبكة الخاصة الافتراضية.

ولكن هذا التخلي عن التحكم المباشر في السياسة الأمنية له عيوبه. خاصة إذا لم يتمكن مقدم الخدمة من تلبية الاحتياجات الأمنية للمؤسسة. وهناك نقطة في غاية الخطورة، وهي أنه إذا تولى مقدم الخدمة مهمة تشفير المعلومات فإن ذلك يعني أن المعلومات ستنتقل من مقر المؤسسة إلى مقدم الخدمة غير مشفرة، والأمر نفسه في رحلة العودة بعد فك شفرتها لدى مقدم الخدمة. هذا الجزء من الرحلة، الذي يكون عادة إما عن طريق خط هاتفي أرضي أو خط لاسلكي، سيصبح هو أضعف أجزاء المنظومة الأمنية. ولتلافي ذلك يقدم بعض مقدمي الخدمة عروضًا تتضمن تشفير البيانات خلال هذا الجزء، برغم أن ذلك يفقد هذا الحل جاذبيته التي كانت تتمثل في البساطة. الأمر الآخر الذي يفتقده هذا الحل هو " المرونة " إذ في بعض الأحوال قد يفرض هذا الحل على المتصلين عن بعد الاتصال عن طريق نفس مقدم الخدمة، ولا يكون لديهم مرونة الاتصال عن طريق مقدمي خدمة آخرين. ولحل هذه المشكلة يضطر مقدم الخدمة لتركيب بعض البرمجيات على أجهزة المستخدمين عن بعد أو يعمد إلى التحالف مع مقدمي خدمة آخرين لتقديم خدمة " التجوال " (Roaming). وبصفة عامة فإن هذا الحل هو الأنسب للشركات الصغيرة، أو يصلح كحل مؤقت للشركات الكبيرة قبل انتقالها للحل الأول [Erbschloe ٢٠٠١]. وهو بصفة عامة يزيح عبئًا كبيرًا عن كاهل مسئولي الأمن في المؤسسات والبنوك [Microsoft ٢٠٠٠].

١٠-٣-٢ اختيار النوع المناسب من الشبكات الخاصة الافتراضية:

عند اختيار نوع الشبكة المناسب يجب أن نأخذ في الاعتبار عدة خصائص يجب أن تتمتع بها الشبكة، منها:

- أسلوب قوي للتحقق من الشخصية.
- أسلوب مناسب للتشفير.

- الالتزام بالمواصفات القياسية.

وفي أحيان كثيرة لا يكون مجال الاختيار واسعًا، فإذا كنت تود الاتصال بمؤسسة أخرى تستخدم نوعًا معينًا من شبكات (VPN)، فغالبًا يتعين عليك استخدام نفس النوع، وأحيانًا يفرض عليك الحل المطلوب نوع جدار الحماية المستخدم في أحد طرفي النفق. ولنتناول الآن الخصائص الثلاث السابق ذكرها بشيء من التفصيل:

١٠-٣-٢-١ أسلوب التحقق من الشخصية:

بدون أسلوب كفء ومتميز للتحقق من الشخصية (Authentication) فلن يكون بمقدورك التأكد من أن الطرف الآخر الذي تتعامل معه عبر نفق الشبكة (VPN tunnel) هو من تظن أن يكون. ويحقق أسلوب " ديفي - هيلمان " (Diffie-Hellman) المستوى المطلوب من خلال تبادل المفاتيح المعلنة.

وينصح " كريس برنتون " في كتابه عن " أمن الشبكات " [Brenton ١٩٩٩] بأنه إذا لم يكن الطرفان اللذان يتبادلان المفتاح العلني يستخدمان إحدى سلطات منح الشهادات الرقمية (Certification authorities)الموثوق بها عند تبادل المفاتيح العلنية عبر شبكة الإنترنت، فلابد أن يتم تبادل هذه المفاتيح عبر وسيلة أخرى مثل الهاتف أو الفاكس.

١٠-٣-٢-٢ أسلوب التشفير:

من المهم أن تحدد المؤسسة مستوى التشفير المطلوب، وهو يتحدد بناء على مستوى الحماية المطلوب، كما يتحدد بناء على العدو المحتمل الذي تود المؤسسة تأمين بياناتها في مواجهته. فالتأمين ضد بعض المخترقين (Hackers) يختلف عن التأمين ضد مخابرات الدول الأجنبية. فقدرات العدو في الحالتين تختلف اختلافًا بينًا. ففي الحالة الأولى ربما كان نظام تشفير (DES) ذو ٤٠ - ٥٦ خانة (Bit) كافيًا تمامًا لإيقاف هؤلاء المخترقين، أما إذا كانت المعلومات المتبادلة أكثر خطورة أو كان العدو أكثر قدرة فربما

احتجنا إلى نظام التشفير الرقمي الثلاثي (Triple DES).

وقد يقول قائل: لماذا لا نستخدم أقوى نظام تشفير ممكن؟ والجواب هو أننا نهتم دائمًا بسرعة الأداء. ففي حالة نظم التشفير القوية ستتأخر عملية التشفير وفك الشفرة إلى الحد الذي قد ينقضي فيه الوقت المسموح به للتطبيق قبل أن يتم التشفير أو فك الشفرة، فتواجهك رسالة (Timeout) الشهيرة. ومن المؤكد أنك إذا كنت تتصل من خلال خط (٥٦ K) باستخدام نظم التشفير (Triple DES) فإنك لن تتمكن من تبادل أي رسائل عبر شبكة (VPN). ففيما يخص أسلوب التشفير ليس الأقوى هو دائمًا الأفضل. كما يؤثر أسلوب التشفير المستخدم على مستوى الأداء، فعادة يستخدم أسلوب (DES) مع شبكات (VPN) بسبب سرعته، أما أسلوب التشفير الذي يستخدم المفتاحين العلني والسري مثل (RSA) الذي يستخدم مفتاحًا بنفس الطول فهو قد يكون أبطأ من عشرة إلى مائة مرة من شفرة (DES)، ذلك لأن أسلوب (RSA) يحتاج وقتًا أطول من المعالج للقيام بالتشفير وفك الشفرة. ومن الناحية العملية فإن كثيرًا من شبكات (VPN)تستخدم أسلوب (RSA) في بداية الاتصال لتبادل المفتاح السري، ثم بعد ذلك تستخدم أسلوب (DES) لتبادل المعلومات.

١٠-٢-٢-٢ الالتزام بالمواصفات القياسية:

من المهم عند اختيار أسلوب التشفير المناسب لشبكة (VPN) التأكد من استخدام خوارزمية (algorithm) معتمدة وموثوقًا بها. فمثلاً استخدام شفرة (DES) بمفتاح طوله ٥٦ خانة (Bit) مثلاً، قد يكون مناسبًا للبيانات العادية، واستخدام الشفرة الثلاثية (Triple DES) التي تستخدم عددًا أكبر من المفاتيح، قد يكون مناسبًا للبيانات الحساسة.

من المهم كذلك التأكد من أن شبكة (VPN) المختارة متوافقة مع باقي الأجهزة المستخدمة. فإذا استخدمت مثلاً نظام (Border Manager) من " نوفيل " في أحد أطراف الشبكة فيجب استخدام نفس النظام في الطرف الآخر.

١٠ ـ ٤ تركيب الشبكة الخاصة الافتراضية:

هناك ثلاثة خيارات يمكن المفاضلة بينها عند تحديد كيفية تركيب الشبكة الخاصة الافتراضية وهي:

- تركيب شبكة تعتمد على جدار الحماية (Firewall-based network)
- تركيب شبكة تعتمد على الموجه (Router-based network)
- تركيب شبكة تستخدم برمجيات أو أجهزة مخصصة لهذا الغرض.

١٠ ـ ٤ ـ ١ شبكة (VPN) المعتمدة على جدار الحماية:

ربما كان هذا النوع هو أكثر أنواع شبكات (VPN) شيوعًا، وذلك لأن جميع المؤسسات تحتاج إلى تركيب جدار حماية على شبكتها في جميع الأحوال، ومن ثم فمن الطبيعي أن يستخدم هذا الجهاز (جدار الحماية) كجزء من شبكة (VPN). ويصبح جدار الحماية بذلك هو النقطة المركزية التي تدار منها شبكة (VPN). العيب الوحيد في هذه الحالة هو بطء الأداء. فإذا كنت تستخدم خط إنترنت محملاً فوق الطاقة وتريد استخدام عدة شبكات (VPN)، وكنت فوق كل ذلك تريد استخدام أسلوب تشفير قوي على جميع هذه الشبكات، وكنت تستخدم كل هذه العمليات من خلال جهاز واحد (جدار الحماية) فلن يكون النظام قادرًا على الوفاء باحتياجاتك، ويكون جدار الحماية في هذه الحالة نقطة الاختناق في النظام. وربما كان هذا هو السبب وراء استخدام بعض جدران الحماية (مثل Firewall-١) لبطاقات التشفير (Encryption cards) لخفض العبء على المعالج. ويتم تركيب هذه البطاقات في إحدى الفتحات الموجودة على اللوحة الرئيسية (PCI expansion slots) بحيث تتولى عمليات التشفير وفك الشفرة لكل البيانات المارة.

١٠ ـ ٤ ـ ٢ شبكة (VPN) المعتمدة على الموجه:

البديل الآخر الذي يمكن أن نفكر فيه هو الموجه (Router) الموجود في مدخل

الشبكة الداخلية للشركة، وهو كذلك من الأجهزة التي تستخدمها الشبكة في جميع الأحوال. واستخدام الموجه سوف يمكننا من فك شفرة البيانات المارة قبل وصولها إلى جدار الحماية. ولما كان بطء الأداء في الشبكات الكبيرة واردًا في هذه الحالة أيضًا، فإن الكثير من أجهزة التوجيه الآن تستخدم دوائر خاصة تسمى " الدائرة المتكاملة المخصصة للتطبيق " (ASIC) أو (Application Specific Integrated Circuit) مما يسمح للموجه بتخصيص بعض المعالجات (Processors) للقيام بمهام محددة، كأن يتم تخصيص معالج معين لفك الشفرة مثلاً، مما يمنع نشاطًا معينًا (مثل فك الشفرة) من تحميل الموجه فوق الطاقة.

العيب الوحيد لهذا النوع هو الأمن! فعادة تكون الموجهات محدودة القدرة على تقديم الأمن المطلوب عند مداخل الشبكة مقارنة بجدران الحماية. فقد يقوم أحد المهاجمين بدس بعض الرسائل من خلال الموجه، وبذلك يظن جدار الحماية أن مصدرها هو الطرف الآخر من نفق الشبكة (VPN tunnel)، وبالتالي يتمكن المهاجم من الوصول إلى بعض الخدمات التي لا يجب أن تستخدم من جانب الغرباء، ويمثل الشكل (١٠-٣) هذه الحالة.

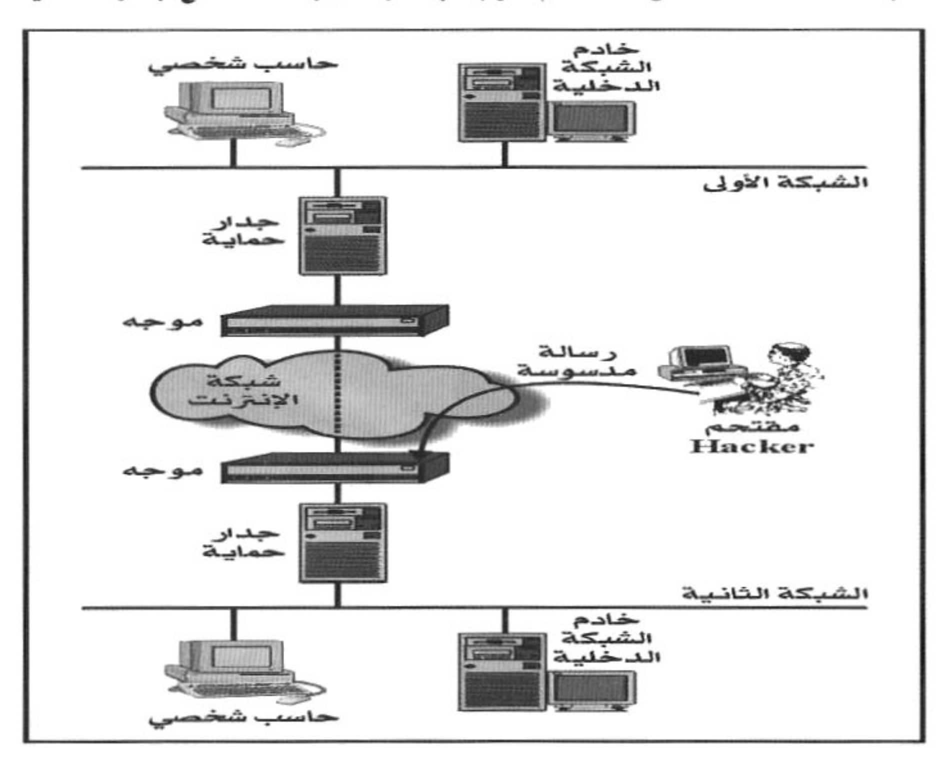
١٠-٤-٣ شبكة تستخدم برمجيات أو أجهزة خاصة:

يمكن استخدام أجهزة أو برمجيات مخصصة لإنشاء شبكة (VPN)، فمثلاً يمكن استخدام جهاز " نفق ألتافسيتا " (Alta Vista tunnel) من شركة (DEC) لإنشاء نفق شبكة (VPN) بين شبكتين محليتين، ويمكن استخدامه مع أي جدار حماية لأنه لا يتدخل في عمل جدار الحماية.

العيب الأساسي في اللجوء لهذا الحل هو إضافة جهاز جديد يحتاج إلى إدارة ويحتاج إلى مراقبة. فإذا تم تركيب هذا الجهاز إلى الخارج من جدار الحماية، أي بحيث يكون جدار الحماية هو الأقرب للشبكة الداخلية فسيكون به نفس العيب الأمني الذي ذكرناه من قبل وهو إمكان دس بعض الرسائل عليه لخداع جدار الحماية مما يشكل ثغرة أمنية حقيقية.

شكل (١٠-٣)

شبكة (VPN) تعتمد على استخدام الموجة وخطر دس رسالة لخداع جدار الحماية

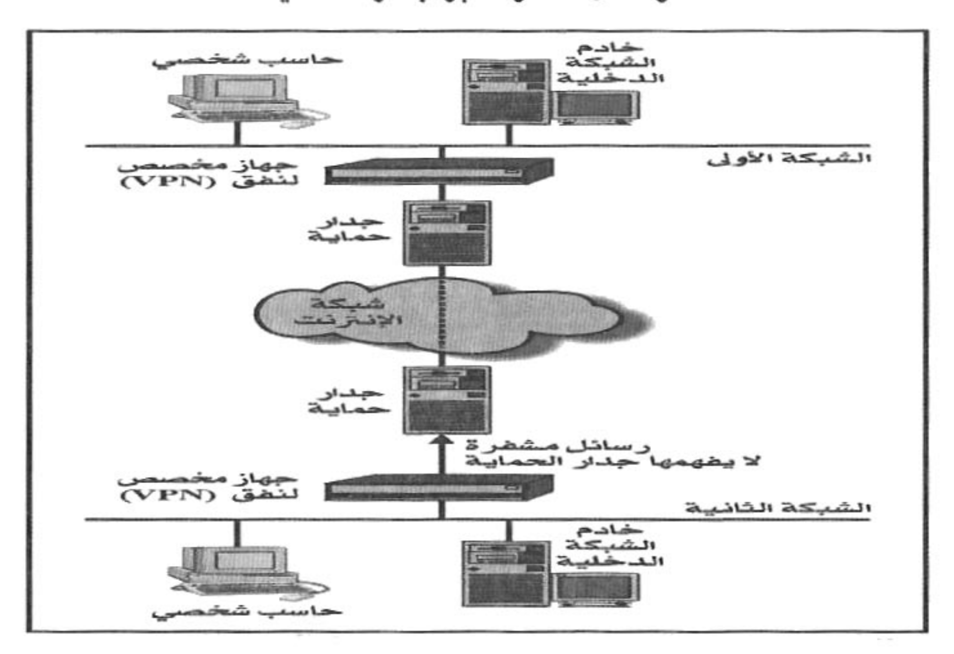


أما إذا وضعنا هذا الجهاز إلى الداخل من جدار الحماية (أي أقرب إلى الشبكة الداخلية)، كما يبدو في الشكل (١٠-٤)، فلن تكون هناك فرصة للاعتماد على السياسة الأمنية التي يطبقها جدار الحماية لأن الرسائل المارة بالنفق لن تمر مفتوحة (غير مشفرة) بجدار الحماية. فالملاحظ أن معظم شبكات (VPN) تقوم بتشفير حزمة الرسالة الأصلية بالكامل، بمعني أن المعلومات المسجلة في مقدمة الحزمة(IP header) ستكون مشفرة ولن تكون متاحة لجدار الحماية ليتخذ القرار المناسب بشأنها. وطالما أن كل الرسائل المارة بين طرفي النفق سيكون لها نفس المقدمة فإن جدار الحماية لن يتمكن من التمييز بين أنواع البيانات (بريد إلكتروني أو استخدام للحاسب عن بعد..)

وسيكون الاعتماد بالكامل على الجهاز المستخدم لشبكة (VPN) ليتولى تحديد نوع الرسائل واتخاذ القرار المناسب بشأنها.

شكل (١٠-٤)

شبكة (VPN) تعتمد على استخدام جهاز مخصص لنفق (VPN) ومرور الرسائل مشفرة عبر جدار الحماية



١٠-٥ اختبار الصلاحية الأمنية للشبكة:

من المهم بعد إتمام تركيب الشبكة الخاصة الافتراضية أن نختبر كفاءتها من الناحية الأمنية. ولإتمام ذلك نقوم بإرسال ملف عن طريق خدمة (FTP) من أحد طرفي النفق إلى الطرف الآخر، ولابد أن يوضح الجهاز المستخدم (سواء كان جدار حماية أو جهاز مخصص) أن الملف المرسل هو ملف مشفر، وأن يوضح العنوان القادم منه الملف، وهو عنوان الشبكة الأولى. يجب كذلك أن نتأكد من أن جدار الحماية (أو غيره) قد قام بفك شفرة الرسالة.

يمكن استخدام " محلل شبكة " (Network analyzer) لتحليل الرسائل المارة بجدار الحماية للتأكد من أن هذه الرسائل قد تم تشفيرها بالفعل، وأنه قد تم فك شفرتها بعد ذلك. سيتولى " محلل الشبكة " إظهار محتويات حزم الرسائل المنقولة، وسيتضح إن كانت مفتوحة أو مشفرة.

يجب كذلك التأكد من عنوان مصدر الرسالة وعنوان مستقبلها (Source and destination IP address) والتأكد من أنها تخص أجهزة شبكة (VPN)، أي أنه لا يجب أن نرى العنوان الحقيقي للشبكة المرسلة أو الشبكة المستقبلة. وهذه من أهم مزايا استخدام شبكات (VPN)، وهنا تكون الشبكة قد اجتازت الاختبار.

بقي أن نؤكد أن تركيب واستخدام شبكات (VPN) يجب أن يكون غير مرئي على الإطلاق من جانب المستفيدين أو من جانب مسئولي الشبكة أو حتى مقدمي الخدمة إذا ما كانت شبكة (VPN) تحت سيطرة مسئول أمن المعلومات في المؤسسة [Kagan ١٩٩٨].

اختتمنا في هذا الفصل حديثنا عن التقنيات المستخدمة في حماية شبكات المعلومات بالحديث عن الشبكات الخاصة الافتراضية. هذا الأسلوب الذي اعتبر فرصة رائعة للعديد من الشركات والمؤسسات لكي تحافظ على أمن معلوماتها المتداولة بين فروعها بأرخص التكاليف.



الفصل الحادى عشر
معالجة الكوارث في شبكات المعلومات



استعرضنا في الفصول السابقة أمن شبكات المعلومات والأخطار التي تتعرض لها هذه الشبكات، ثم تقنيات الحماية المتوفرة بكافة أنواعها، وكيفية استخدامها بالشكل الذي يؤمن شبكات المعلومات ضد الاختراق.

والآن نخصص هذا الفصل قبل الأخير من الكتاب لمعالجة الكوارث بعد حدوثها في شبكات المعلومات. ونركز في معالجتنا للكوارث على تلك الكوارث التي يسببها البشر، أي الناجمة عن الاختراق والانتهاك المتعمد لشبكات المعلومات، فنبدأ بالحديث عن بعض الإجراءات الواجب اتباعها مسبقًا للحيلولة دون تفاقم آثار الانتهاك، وللإسراع في عمليات استعادة الوضع التي تعقب الكارثة.

نتحدث في القسم الثاني عن عملية مهمة وهي ملاحقة المجرم واقتفاء آثاره والتعاون في هذا الصدد مع مواقع أخرى قد يكون المجرم استخدمها كنقطة وثوب لاختراق شبكتنا.

في القسم الثالث نحدد الخطوات اللازم اتباعها عند وقوع الانتهاك، وأهمية كل خطوة، والبدائل المتاحة فيها.

الكثير من المؤسسات تبدأ التفكير في كيفية معالجة كوارث أمن المعلومات (بعد) أن تقع الكارثة، أي بعد وقوع الفأس في الرأس. ولكن إذا كان لدى المؤسسة خطة مسبقة لكيفية معالجة الكوارث في الشبكة فإن ذلك سيوفر عليها ضياع وقت ثمين فور وقوع اقتحام للشبكة، وبعد حدوث عرقلة الخدمة، وهو الوقت اللازم لوضع تصور عما يجب القيام به لاستعادة الوضع إلى ما كان عليه، ولملاحقة المجرمين، ولتقليل آثار المشكلة.

وربما كان أفضل النصائح التي توجه لمسئولي الأمن عما يجب فعله عند حدوث الكارثة هي:

(١) تماسك وتجنب الذعر.

(٢) اهتم بتوثيق كل شيء [Garfinkel ١٩٩٦]

١١ ـ ١ الاستعداد لمواجهة الكوارث في شبكات المعلومات:

من المهم أن يتم اتخاذ بعض الإجراءات المسبقة في المؤسسة استعدادًا لمواجهة كوارث اقتحام الشبكة، وهي:

١١ ـ ١ ـ ١ النسخ الاحتياطي:

أهم جزء في رحلة استعادة النظام بعد حدوث الاختراق، هو استعادة البيانات المفقودة أو المزورة من النسخ الاحتياطية السابق الحصول عليها على فترات زمنية محددة ومتقاربة. ولذلك فخطة النسخ الاحتياطي يجب أن تكون سليمة ومعدة بعناية، كما يجب أن يتم اختبارها باستمرار. وفي كثير من الجهات، وبعد شهور طويلة من العمل، يتم اكتشاف أن هذه الجهة لم يكن لديها أي نسخ احتياطية على الإطلاق عبر هذه الشهور. ذلك إما بسبب تلف الوسط الذي كان يتم عليه تخزين النسخة الاحتياطية، أو بسبب خطأ الإجراءات المستخدمة في عمليات النسخ الاحتياطي.

١١ ـ ١ ـ ٢ مخطط الشبكة:

من الأمور الهامة التي قد تظهر الحاجة إليها بشدة خلال عملية استعادة الوضع بعد الكارثة هي اللجوء إلى مخطط الشبكة. هذا المخطط يبين مواقع أجهزة الخدمة (Servers)، ومواقع أجهزة الحاسب، ومواقع أجهزة أمن المعلومات، مثل جدران الحماية وخوادم البروكسي وأجهزة كشف الاقتحام. كما يجب ترقيم كل هذه الأجهزة على مخطط الشبكة، ولصق بطاقات تمييز على الأجهزة نفسها تحمل هذا الترقيم. هذا سيسهل إلى حد كبير تتبع مسار كثير من حزم الرسائل، كما أنه سيكون ذا فائدة جمة عند غياب مسئول الشبكة وعدم وجود من يعرف تفاصيل الشبكة.

يمكن كذلك إعداد بطاقات لكل نظام تصف النظام، ونسخته، وأسلوب التهيئة المتبع، وكمية الذاكرة التي يستهلكها، والمساحة التي يحتلها على القرص، والمسئول عن هذا

النظام. هذه البطاقات يمكن إعدادها كذلك لكل جهاز (ويفضل لصقها على الجهاز نفسه)، كما يجب تحديث هذه البطاقات للنظم والأجهزة من وقت لآخر.

١١ـ١ـ٣ قيم المجموع الاختباري (Checksum):

تحدثنا من قبل في الفصل الخامس من هذا الكتاب (أساليب انتهاك شبكات المعلومات) عن استخدام " المجموع الاختباري " (Checksum) كوسيلة للتأكد من أن الملفات لم يحدث عليها تعديل أو تحريف. ومن المهم بعد حدوث الاختراق أن نتأكد من أن ملفات المؤسسة لم تتعرض لشيء من ذلك. ولكن نظم التشغيل المعروفة لا تستخدم وسائل متقدمة لإعداد قيم المجموع الاختباري. ومن ثم فقد يعمد المهاجم إلى اصطناع قيمة المجموع الاختباري، وإلى إعادة تاريخ تعديل الملف إلى ما كان عليه في السابق، من باب التضليل.

لذلك فمن المهم حصول المؤسسة على برنامج مشفر للمجموع الاختباري (Cryptographic Checksumming Program)، ومن خلال هذا البرنامج يتم إعداد المجموع الاختباري للملفات الهامة في النظام على فترات (على أن تكون هي نفس فترات إعداد النسخ الاحتياطية)، والاحتفاظ بقيم المجموع الاختباري في مكان آمن خارج الجهاز (Offline)، حتى لا يتمكن المهاجم من التلاعب بهذه القيم.

١١ـ١ـ٤ سجل التعديلات:

سجل التعديلات يتم فيه تسجيل أي تعديل يجري على النظام، سواء قبل حدوث الانتهاك أو خلاله أو بعده. وهذا السجل يتم الرجوع إليه لتحديد البرامج التي تم تركيبها، والتعديلات التي تمت على تهيئة الأجهزة، أو لمعرفة الأجهزة التي تمت إضافتها للشبكة مؤخرًا.

من خلال هذا السجل يمكن بسهولة " التراجع " عن التعديلات التي تمت، إذا ثبت

خطؤها. كما يمكن من خلاله اكتشاف أي تعديل من التعديلات هو الذي تسبب في عدم إمكان إعادة تشغيل أحد النظم مثلاً. وفي كثير من الأحيان يجد مسئول الشبكة نفسه أمام برامج أو أجهزة لا يعلم من أين جاءت، ومن خلال هذا السجل يستطيع أن يقطع الشك باليقين. وربما كان أسهل أسلوب للاحتفاظ بهذا السجل هو إرسال رسالة بريد إلكتروني لشخص آخر (أو اسم وهمي) عند إجراء كل تعديل، ومن فحص بريد هذا الشخص بعد ذلك يمكن الحصول على قائمة كاملة بكل التعديلات التي تمت وتواريخها.

١١ - ١ - ٥ التزود بالمعدات مسبقا:

يجب أن يكون لدى المسئولين عن الموقع مسبقًا وقبل حدوث الكارثة كل البرامج والأقراص والمعدات التي قد يحتاجون إليها عند حدوث الانتهاك، بدلاً من البحث عنها في الأوقات العصيبة. ومن هذه الأدوات:

- أشرطة وأقراص خالية للنسخ الاحتياطي.
- بعض العدد والأدوات التي قد يحتاجون إليها عند الفصل الفعلي لبعض الخطوط (وربما سلم متنقل إذا كانت الخطوط تمر في السقف).
- بعض الكابلات الإضافية ووصلات الكابلات.
- جهاز حاسب دفتري (Notebook)مؤمَّن ومضمون عدم اختراقه، لعدم سابق ارتباطه بالشبكة.

١١ - ١ - ٦ بعض الطرق الآمنة لاختيار كلمة السر:

يمكن اتباع عدة أساليب حتى يمكن تحجيم قدرة المهاجمين على تخمين كلمة السر وضمان عدم كشفها من جانب البرامج الخاصة باكتشاف كلمات السر.

تعتبر أفضل وسيلة للدفاع في مواجهة برامج التخمين العشوائي لكلمات السر هي استخدام كلمات سر قوية لا يسهل تخمينها، كما يمكن استخدام نظام كلمة السر لمرة

واحدة والذي يتطلب تغيير كلمة السر في كل مرة يدخل فيها المستفيد إلى النظام. وهناك بعض البرامج المجانية (Freeware)التي تجعل عملية التخمين العشوائي أكثر صعوبة وأقل فاعلية ونذكرها في جدول رقم (١١ - ١).

جدول رقم (١١ - ١)
بعض البرامج المجانية لتأمين كلمة السر

البرنامج المجاني	وصف البرنامج	مكان الحصول عليه
S/key	نظام يستخدم كلمة السر لمرة واحدة.	http://www.yak.net/skey/
OPIE	نظام يستخدم كلمة السر لمرة واحدة.	ftp.nrl.navy.mil/pub/security/opie
Cracklib	أداة استقبال كلمة السر من المستفيد.	ftp://ftp.cert.org/pub/tools/cracklib/
Npasswd	تعمل لهذه الأداة كبديل للأمر Passwd	http://www.utexas.edu/cc/unix/ software/npasswd
Secure Remote Password	نظام للتحقق من الشخصية وتبادل مفاتيح التشفير عبر الشبكة.	http://srp.stanford.edu/srp
SSH	تعمل هذه الأداء كبديل للأمر R مع التشفير واستخدام أسلوب (RSA) للتحقق من الشخصية	

بالإضافة إلى هذه الأدوات (أو البرامج) فمن المهم اتباع الإجراءات التالية لضمان استخدام كلمات سر قوية وهي:

(١) يلزم التأكد من أن جميع المستفيدين لديهم كلمات سر.

(٢) يجب فرض تغيير كلمة السر كل ٣٠ يومًا للمستخدمين ذوي الصلاحيات العالية، وكل ٦٠ يومًا للمستخدمين العاديين.

(٣) يجب ألا يقل عدد أحرف كلمة السر المستخدمة عن ستة أحرف، ويفضل أن تكون من ثمانية أحرف.

(٤) يمكن إعداد البرنامج الذي يستخدمه المستفيد لإدخال كلمة السر بحيث لا يقبل من المستفيد كلمات السر البسيطة.

(٥) يجب نصح المستفيد بعدم استخدام نفس كلمة السر في كافة الأنظمة التي يدخل إليها المستفيد.

(٦) يجب نصح المستفيد بعدم كتابة كلمة السر الخاصة به وعدم إفشائها للآخرين.

(٧) استخدام كلمات السر التي يلزم تغييرها عند كل دخول للنظام إذا أمكن ذلك.

(٨) على رأس هذه القائمة تأتي أهمية التأكد من أن بعض رموز المستفيدين (User ids) ذات الصلاحيات العالية مثل (admin) أو (setup) لا تحتفظ بكلمات السر التلقائية (default) التي تأتي مع النظام عند تركيبه، وفي هذه الحالة يجب تغيير كلمات السر هذه لأنها تكون معروفة للجميع.

١١ ـ ٢ معالجة الكوارث التي تصيب مكونات الشبكة أو أجهزة الخدمة:

تتطلب معالجة الكارثة تنفيذ مجموعة من الخطوات. هذه الخطوات ليس من الضروري أن نحتاج إليها جميعًا، ولكن عند التخطيط المسبق يجب أن نعد لكل احتمال عدته. كما يجب أن تحدد الخطة في كل خطواتها الشخص المسئول عن تنفيذ هذه الخطوة، والأشخاص المطلوب إبلاغهم، وكيفية الاتصال بهم. وسوف نركز هنا على كيفية مواجهة الكوارث الأمنية، أي التي تنتج عن عمليات انتهاك أو اقتحام، وليس أي كوارث أخرى.

١١ ـ ٢ ـ ١ تقييم الموقف:

يجب في هذه الخطوة البدء بالإجابة فورًا عن سؤالين مهمين:

[١] هل نجح المهاجم في الوصول إلى النظم المطلوب حمايتها؟

[٢] هل الهجوم مستمر وقائم حاليًا أم انتهى؟

وبناء على الإجابة عن هذين السؤالين فقد يكون التصرف المطلوب حاسمًا مثل: فصل الشبكة عن الإنترنت، أو إيقاف أجهزة الخدمة عن العمل. أو قد يكون التصرف المناسب أقل حدة كأن نترك المهاجم في محاولاته، إذا كنا متأكدين من أنه لن ينجح فيها، أملاً في الإمساك به متلبسًا. ولكن السؤال المهم هو من الذي يتخذ هذا القرار؟ من الذي يقرر التصرف المناسب؟ يجب مسبقًا تحديد اسم هذا المسئول، واسم مسئول بديل في حالة عدم وجوده. وفي المؤسسات الكبيرة يمكن تحديد المسئول بالوظيفة التي يشغلها وليس بالاسم.

قبل الذهاب إلى أبعد من ذلك في خطوات مواجهة الكارثة يجب البدء فورًا في " التوثيق ". وليس من المتوقع أن يكون التوثيق كاملاً في هذه اللحظات العصيبة، وإنما يمكن أن يتم كرؤوس موضوعات فقط يتم استكمالها فيما بعد.

١١ـ٢ـ٢ اتخاذ القرار:

في هذه الخطوة يتم اتخاذ القرار المناسب كما أسلفنا. وفي كثير من الأحيان يؤدي فصل الجهاز الذي وقع عليه الاختراق عن الشبكة إلى إيقاف الهجوم وتمكين باقي المستفيدين من الاستمرار في استخدام الشبكة، ولكن ذلك سيجعل من الصعب تعقب المهاجم، فالصلة ستنقطع بين الشبكة والمهاجم، وإن كانت البرامج التي قد يكون المهاجم زرعها في الشبكة مستمرة في العمل ومازال تتبعها ممكنًا. ولكن في كثير من الأحيان قد يكون قطع الاتصال بشبكة الإنترنت هو الحل المناسب.

قد يكون الملجأ الأخير هو إيقاف العمل بالشبكة بالكامل، وقد جعلناه ملجأ أخيرًا لأنه سوف يقضي على المعلومات التي قد يحتاجها المسئول في تحليل الحادث، كما أنه سيعطل الكثيرين من مستخدمي الشبكة عن عملهم.

كما ذكرنا سابقًا فإن هذه الاختيارات والبدائل يجب أن يكون مخططًا لها من قبل، حتى يتم اتخاذ القرار السليم بالسرعة المناسبة. ولكل موقع ظروفه التي تفرض عليه اختيارًا معينًا. ففي الشبكات الكبيرة النشطة قد يكون إيقاف الشبكة بالكامل عن العمل أمرًا مستحيلاً، مثلما هو الحال في شبكات شركات الطيران، وشبكات الجوازات، وبعض مواقع الخدمات الهامة كشبكة البنوك وغيرها. وقد يكون الأمن والخشية على البيانات أكثر أهمية، بحيث يجب إيقاف الهجوم بأي ثمن. وقد يكون الإمساك بالجاني أكثر أهمية من كل ما سبق (إذا كانت المؤسسة قد اتخذت احتياطاتها وأمنت دفاعاتها بشكل جيد، وأصبحت على ثقة من عدم تمكن المهاجم من الوصول إلى البيانات السرية)، فترك الحبل للمجرم في هذه الحالة قد يكون هو القرار السليم.

يجب أن تتضمن خطة مواجهة الكوارث كيفية فصل الشبكة، والخطوات التي يجب اتباعها لإيقاف الأجهزة عن العمل. فهذا الأمر يجب أن يتم بشكل مخطط وليس بقطع الكهرباء عن المبنى ! ومن ناحية أخرى، فالمؤسسة لا تود أن تسمح بالإغلاق الروتيني العادي الذي يمنح المهاجم خمس عشرة دقيقة إضافية. ولذلك يمكن أن نضع البديلين التاليين:

في معظم حالات الطوارئ الأمنية الحادة يفضل إغلاق الأجهزة إغلاقًا فوريًا ولكن منتظمًا (Graceful shutdown) دون إرسال تحذير للمستفيدين.

إذا كان المهاجم يقوم بالفعل بتدمير البرامج والملفات فإن الحل المناسب هو قيام المستفيدين بإغلاق أجهزتهم فورًا بأسرع وسيلة ممكنة وذلك بقطع الكهرباء فورًا عن الأجهزة حتى لو سبب ذلك لها ضررًا، فالضرر في هذه الحالة سيكون أهون.

١١-٢-٣ البدء في إجراءات الحل:

في هذه الخطوة نبدأ في إصلاح ما فسد. ويتطلب ذلك أعصابًا هادئة ومعرفة بحقيقة ما حدث، حتى لا نزيد الأمر سوءًا. ويفضل أن يقوم بالعمل شخصان يراجع

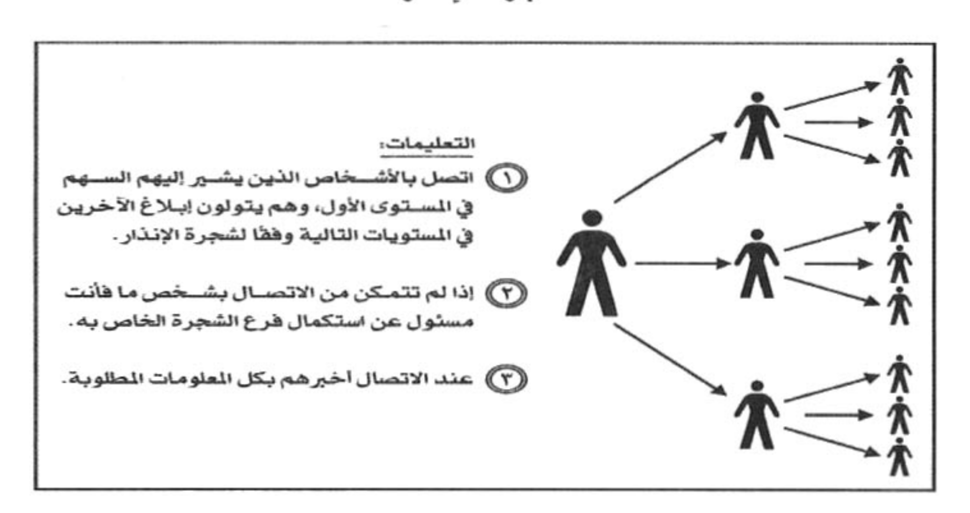
كل منهما ما يقوم الآخر بإصداره للشبكة من تعليمات، وما يقوم بتشغيله من برامج. كما يجب أن يتفادى مسئول الأمن ومسئول الشبكة اللذان يعالجان الوضع التعامل مع المستفيدين والرد على أسئلتهم، بل يفضل تخصيص شخص آخر لهذه المهمة.

١١-٢-٤ الإبلاغ عن المشكلة:

لابد في هذه الخطوة من إبلاغ كثير من الجهات عن هذا الاختراق الأمني، ومن هذه الجهات:

[١] يجب إخطار إدارة المؤسسة والمستفيدين بها بالموقف وبما يمكن أن يمدوا به يد العون للفريق الذي يقوم بالتصدي للحادث، على الأقل لضمان عدم قيام أحد بعرقلة جهود الفريق، كأن يلاحظ شخص ما قطع التيار المتعمد عن الأجهزة فيتطوع لإعادة التيار وتشغيل الأجهزة ! كما يجب في بعض الأحيان إخطار إدارة العلاقات العامة والإدارات المختصة بالشئون القانونية والشئون الإدارية.

شكل (١١-١)
شجرة الإنذار



ولا بد من إعداد قوائم بأرقام الهواتف وأسماء الأشخاص الذين يجب الاتصال بهم في هذه الإدارات والجهات، ويمكن استخدام " شجرة الإنذار " للاتصال بهؤلاء الأشخاص، كما يبينها الشكل (١١-١)، بحيث تكون مهمة كل شخص الاتصال بمجموعة من الأشخاص لا تزيد عن ثلاثة. وبذلك يمكن توصيل الرسالة لأكبر عدد من الأشخاص في أقصر وقت. ولا يشترط أن تعكس هذه الشجرة أي ترتيب إداري أو تنظيمي في المؤسسة. كما يجب أن تكون الرسالة المبلغة واضحة وشاملة، ويمكن إعداد نص مسبق لهذه الرسالة يمكن استخدامه، بعد تعديله، وفقًا للظروف.

وبعض الجهات تستخدم شفرة رمزية للإخطار بأن هناك هجومًا وقع وأن الخدمة ستتوقف، وهذه الشفرة قد تكون مثلاً " سيتم الاجتماع الموسع مع المدير العام خلال عشر دقائق ". ويفهم الجميع من هذه الرسالة أن هناك هجومًا يتم في هذه اللحظة على الشبكة وأن على المستفيدين إغلاق أجهزتهم لأن الشبكة سيتم فصلها خلال عشر دقائق.

[٢] يجب إخطار الشركة الموردة، والشركة (أو الشركات) التي تتولى تقديم خدمة الإنترنت للمؤسسة، وذلك لاحتمال الحاجة إلى مساعدتهم في علاج آثار الحادث. وربما أدى هذا التحذير لمقدم الخدمة إلى إنقاذ مواقع أخرى معرضة للهجوم، إذ ربما كان مقدم الخدمة يتعرض هو نفسه للهجوم. كما أن الكثيرين من مقدمي الخدمة والشركات الموردة لنظم التشغيل وللنظم الأمنية يكون لديها نصائح هامة وأدوات معينة في مثل هذه الأحوال، من واقع خبرتهم بالنظم المستخدمة، ومن واقع تجربتهم الطويلة. هذه النصائح قد تكون مفيدة للمؤسسة.

[٣] يجب الاتصال بأي مواقع أخرى قد يكتشف أنها أيضًا عرضة للهجوم، أو قد يكتشف أن أحد المستفيدين بها متورط في هذا الهجوم. وهذا الاتصال يمكن تأجيله بعض الشيء لحين الانتهاء من إعادة الأمور إلى نصابها.

يجب كذلك الاتصال بالمواقع التي تشكل جزءًا من شبكة المؤسسة، مثل حالة استخدام الشبكة الخاصة الافتراضية، فالأطراف الأخرى التي تضمها هذه الشبكة

الافتراضية عليهم أن يعلموا بالاختراق الذي حدث وبما يتم من إجراءات.

١١ـ٢ـ٥ إعداد نسخة احتياطية لحظية:

يجب الحصول على نسخة احتياطية تمثل اللحظة التي تم فيها الاختراق أي " نسخة احتياطية لحظية " (Snapshot) ويمكن إتمام ذلك بإعداد النسخة الاحتياطية على شريط، أو على قرص آخر. وأهمية إعداد هذه النسخة تظهر إذا تم تشخيص المشكلة بشكل خاطئ، أو إذا تم اتخاذ إجراءات أفسدت البيانات، فيمكن الرجوع إلى النسخة الاحتياطية وإعادة هذه الإجراءات مرة أخرى. كما أن هذه النسخة سيكون استخدامها مفيداً في التحقيقات والفحوص اللاحقة لتتبع المجرم دون خوف من إفساد دليل الإدانة [Icove ١٩٩٥].

١١ـ٢ـ٦ استعادة الوضع:

الخطوة الهامة (قبل الأخيرة) هي استعادة الوضع، وإعادة الخدمة للمستفيدين، وإعادة قواعد البيانات لما كانت عليه. ويتوقف ما يتم عمله في هذه الخطوة على مدى الضرر الذي وقع على النظام، وهل نجح المهاجم في إلحاق الأذى بأصول المؤسسة أم لا؟

ومن الصعب توقع خطوات استعادة النظام مسبقاً. لأنها تختلف بشكل كبير من حالة إلى أخرى. فقد يصل الأمر إلى إعادة بناء النظام بالكامل من جديد، ولكن النصيحة الهامة في هذه الحالة هي ضرورة فحص النظام جيداً، لأنه في معظم الأحوال يترك المهاجم خلفه في النظام الضحية خطاً للرجعة، أو " باباً خلفياً " (Back door)، لكي يتمكن من العودة مرة أخرى بسهولة. ومن ثم فعند إعادة بناء النظام يجب التأكد من سلامة كل مكوناته، ويفضل استخدام النسخة الاحتياطية المأخوذة قبل الحادث.

١١ـ٢ـ٧ توثيق الحادث:

هذه هي الخطوة الأخيرة والتي ربما تتم في بحبوحة من الوقت بعد التخلص من

التوتر. في هذه الخطوة يتم توثيق كل ما تم اكتشافه من وقائع، وما تم اتخاذه من إجراءات. ويفيد ذلك في اكتشاف مدى الضرر الذي حدث، وفي اتخاذ الإجراءات التي تضمن عدم تكرار هذا الحادث. كما تفيد في حالة إقدام المؤسسة على ملاحقة الجناة قضائيًا.

يفضل أن يكون التوثيق من خلال أوراق مستخرجة من الحاسب وموثقًا عليها تاريخ استخراجها (فالمعلومات المخزنة على الحاسب يمكن اختراقها وتزويرها). وربما كانت المعلومات التالية من بين التوثيق المطلوب إعداده:

- الاتصالات التي تمت وتوقيتاتها وأطرافها، وملخص ما تم فيها.
- الاجتماعات واللقاءات والقرارات الهامة التي تم اتخاذها مثل توقيت فصل الشبكة.
- أي مشاكل قد تكون اعترضت الخطة الموضوعة مسبقًا، مثل اكتشاف أن النسخة الاحتياطية غير سليمة.
- سجل الوقائع وهو من أهم الوثائق المفيدة.

١١-٢-٨ الخطوة ما بعد الأخيرة:

بعد انتهاء الحادث وتجاوز آثاره وتوثيق وقائعه، يجب التفكير بهدوء شديد، ومحاولة فهم ما حدث بالضبط، وتحديد الإجراءات المطلوب اتخاذها مستقبلاً لمنع تكراره. وهنا يمكن فحص النسخة الاحتياطية اللحظية (Snapshot) التي تم الحصول عليها خلال إجراءات مواجهة الكارثة. ومن المؤكد أنه ستظهر في هذا الوقت بعض التعديلات الواجب إدخالها على خطة مواجهة الكوارث، وربما على العديد من الإجراءات المتبعة في المؤسسة. يجب كذلك تحليل الإجراءات التي تم اتخاذها فور وقوع الكارثة، لمعرفة هل كانت هذه الإجراءات سليمة؟ أم أن هناك " دروسًا مستفادة ".

وفي النهاية يجب إعادة الاتصال بكل من تم إبلاغهم من قبل بوقوع الكارثة لإبلاغهم بأن كل شيء الآن على ما يرام، وربما كذلك لإبلاغهم بأي إجراءات جديدة أو تعليمات للمستقبل.

١١ ـ ٣ مثال لأحد التطبيقات العملية لمعالجة الكوارث:

من أهم فوائد عملية معالجة الكوارث هو منع تكرار وقوعها، ومن أهم ما يمكن عمله لتحقيق هذا الهدف هو الإمساك بالمجرم الذي تسبب في الكارثة. ولذلك كانت ملاحقة المجرم من أهم التطبيقات العملية لمعالجة الكوارث.

١١ ـ ٣ ـ ١ ملاحقة المجرم:

كأي جريمة، تحتاج جريمة انتهاك أو اقتحام شبكة المعلومات إلى ملاحقة المجرم، وجمع الأدلة ضده، والإمساك به، وتقديمه إلى المحاكمة. ولكن هل هذه العملية سهلة؟ أم تكتنفها الصعوبات؟

من المؤكد أن هذه العملية يمكن أن تستغرق شهورًا طويلة، ربما سنة أو أكثر، إلا إذا لعبت المصادفة دورها، أو كان المجرم على درجة كبيرة من الغباء. وليست المدة وحدها هي المطلوبة، ولكن ينتظر القائمين بهذه المهمة جهد كبير وعمل روتيني شاق، يتمثل في فحص آلاف الوقائع، وتتبع آلاف حزم الرسائل، والاصطدام في عشرات المرات بباب مسدود مما يعني حتمية العودة للبدء من جديد. ونحن هنا نفترض أن هذا العمل سيقوم به مجموعة من الباحثين وليس شخصًا بمفرده، وربما احتاج الأمر إلى التعاون بين مسئولي أمن المعلومات ومسئولي الشبكة وبعض جهات البحث الجنائي لكي يتم التعامل بحذر مع الأدلة المختلفة.

١١ ـ ٣ ـ ٢ المشاكل التي تواجه المحقق في ملاحقة المجرمين:

هناك مشكلة فنية هامة تواجه المحقق خلال محاولته ملاحقة المجرم، وهي أن تتبع مصدر الهجوم إلى جذوره أمر صعب للغاية، فمن السهل معرفة " الموقع " أو الشبكة التي جاء منها الهجوم، وذلك بفحص عنوان المصدر الموجود في حزم الرسائل (IP address). ولكن هذا العنوان في معظم الأحوال لن يكن هو مصدر الهجوم، وإنما

هـو كما ذكرنا من قبل، ليس إلا نقطة وثوب استخدمها المهاجم بعد أن قام باختراق هذا الموقع الذي لا يعدو كونه ضحية أخرى للمجرم. وبالتعاون مع المسئولين في هذا الموقع الضحية (والتعاون مهم لتسهيل التتبع) سوف نكتشف سريعًا أن المصدر هـو حلقة أخرى في سلسلة الضحايا. هذه السلسلة التي يتعمد المهاجمون إطالة حلقاتها حتى يصعب الوصول إليهم. وهناك من الناحية العملية حد أقصى لعدد المواقع التي يمكن تعقبها خلال اقتفاء أثر المجرم خلال مدة زمنية معقولة.

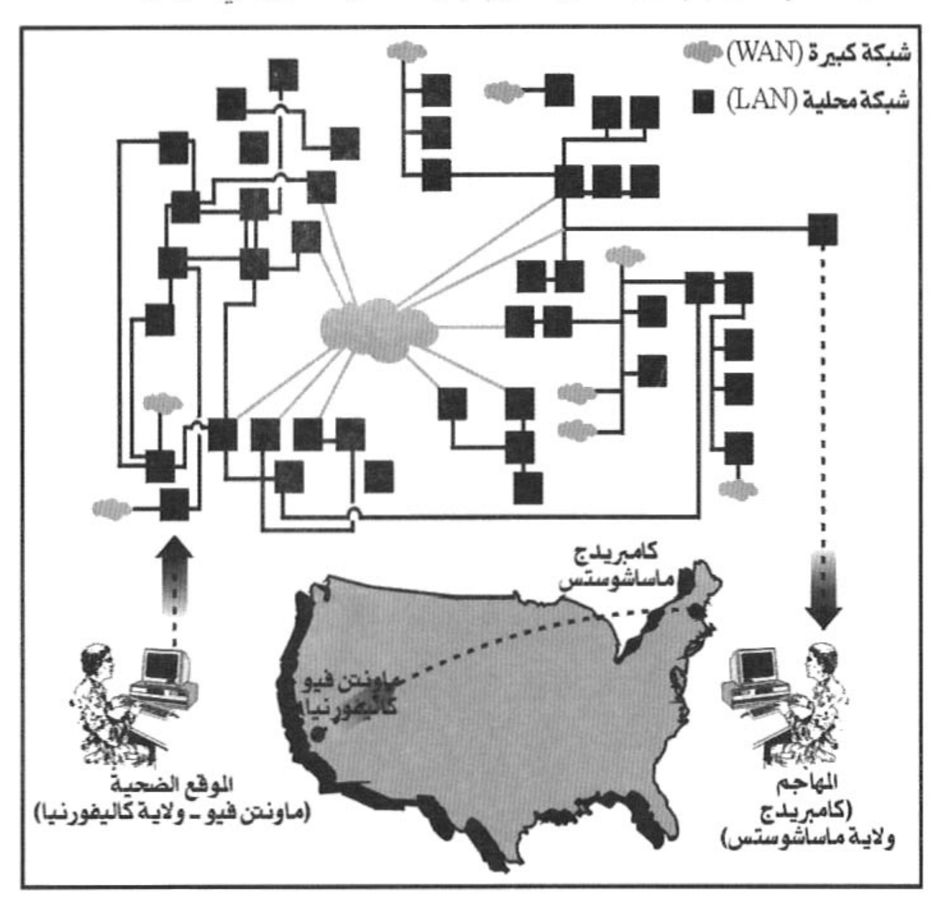
وهناك أيضًا صعوبة أخرى وهي احتمال عدم تعاون بعض المواقع خلال هذه السلسلة، إما بسبب عدم وجود خبراء لديهم، أو عدم وجود وقت كاف، أو ربما كانوا غير مهتمين بهذا الاختراق، أو كانوا من الجهات التي تؤثر الصمت والتكتم على هذه الاختراقات.

ربما كذلك يجد المسئول من بعض المواقع استجابة سلبية أو عدائية، أو قد يصادف بعض المواقع التي تتلقى مثل هذه الشكوى بشكل يومي، أو ربما يجد المسئول على الطرف الآخر من لا يفهم المطلوب أو من لا يفهم المشكلة برمتها، أو ربما يجدهم يدعونه لكي يحضر إليهم ويقوم بمهمة التتبع بنفسه، وهذا مستحيل بالطبع.

من المشاكل التي تواجه المحقق في اقتفاء آثار المجرم أن يكتشف في بعض حلقات السلسلة أن المهاجم قد اتصل من خط هاتفي، وتتبع المكالمات الهاتفية أمر تكتنفه العديد من العوائق الفنية والقانونية. ويمثل الشكل (١١-٢) عملية تعقب لمجرم من الموقع الضحية في "ماونتن فيو" بولاية كاليفورنيا في أقصى الغرب الأمريكي إلى " كامبريدج " بولاية ماساتشوسيتس في أقصى شرق الولايات المتحدة، مرورًا بالعديد من الشبكات المحلية والشبكات الكبيرة [Zwicky ٢٠٠٠].

شكل (١١-٢)

مثال لتعقب المهاجم من أقصى الغرب إلى أقصى الشرق في الولايات المتحدة



هناك نقطة هامة أخرى نود أن نوجه إليها عناية القائم بتتبع الأثر، هي أنه عند الاتصال بمواقع أخرى في سلسلة الاختراقات، كيف تكون متأكداً من أنك قد اتصلت بالفعل بالمسئول الحقيقي عن الموقع؟ ألا يحتمل أن من تلقى بريدك الإلكتروني وقام بالرد عليه هو المقتحم نفسه الذي يضع نفسه في مسار أي اتصال مع الموقع الضحية؟ وحتى لو تأكدت أنك تتخاطب بالفعل مع المسئول الحقيقي عن الموقع، من أدراك أن هذا المسئول " الحقيقي " ليس هو نفسه المهاجم الذي تبحث عنه؟!!

النقطة الأخرى التي نود أن ننبه إليها المسئول عن الموقع هي أنه عند اكتشاف تورط أحد المواقع في الهجوم، فينبغي الاتصال بهذا الموقع وتوضيح المشكلة للمسئولين فيه وإمدادهم بالمعلومات التي سوف يحتاجون إليها لتتبع المجرم، مع الوضع في الاعتبار أن هذا الهجوم ربما كان مجرد خطأ من مستفيد لم يحسن استخدام التعليمات.

الفصل الثانى عشر
تقييم مستوى الأمن في نظم تشغيل الشبكات

في هـذا الفصل الأخيـر من كتـاب " أمن شبكـات المعلومـات " ، وبعد أن تعـرفنا في الفصول السابقة على الأخطار والمشـاكل الأمنية التي تواجه الشبكات وكيفية مواجهتها والحمايـة منهـا، نتعـرض لموضـوع هام يـتعلق بمدى تمـتع نظم التـشغيل، أو قل بـيئات التشـغيل المنتـشرة هـذه الأيام، بـالأمن. وكيـف يمكن تحسـين مستـوى الأمن فيـها من خلال التدقيق عند تهيئة هذه النظم؟

القسـم الأول من هذا الفصل يتعامل مـع نظام " نتوير " (NetWare) فـيبدأ بالحديث عن صلاحيات المستفيدين في استخدام الملفات وكيفية منح هذه الصلاحيات، ثم بكيفية إدارة حسابات هؤلاء المستفيدين، وبعد ذلك يبين كيف يتم تأمين الاتصالات عبر الشبكة في هذا النظام، ويشرح بعـض الأدوات الإضافية المتاحة لمدير الـنظام التى تساعده على تحسين مستوى الأمن فيه.

القسـم الثـانـى يتعـامل مع نظـام " ونـدوز إن تي " (Windows NT) فنبـدأ كذلك بالحـديث عن صلاحيـات استخدام الملفـات، ثم حسـابات المسـتفيدين، حـيث نبين بعض خصـائص هـذا الـنظـام مثـل: " المميـز الأمني "(SI)، و " مـديـر الحسـابـات الأمني " (SAM) ثم نتحدث عـن نظام " مراقبـة الوقائع " (Event Viewer)، و " تـصفية الحزم " (Packet Filtering) ثم نتحدث عن الجيل الجديد من هذا النظام وبالذات عن " الدليل النـشط "(Active Directory) الـذى تعـول عليه شـركـة " مـايكـروسـوفـت " كثيـرًا في الترويج لمنتجات (SQL Server) وما يصاحبها من خدمات.

القسم الثـالث خصصـناه لنظـام " يونكـس " الذي لا يزال يـتمتع بشعـبية كبـيرة فى الشبكات المرتبطة بشبكة الانترنت، وفى الكثير من الجـامعات. فنتحدث بنفس النمط عن صلاحيـات الملفات وحـسابـات المستفـيدين. ونـركز علـى أسلوب " يـونكس " فـى ترك كلمـات السر المشفرة قابلـة للقراءة، وكيف يـواجه النظام هـذه النقطة بـاستخدام ملف " الظل "(Shadow).

إنني علـى ثقة من تفـهم القارئ الكريم للصعوبـة البالغـة التى تكتنف هذه المحـاولة

لتقييم نظم تشغيل الشبكات من ناحية الأمن. وهذه الصعوبة لها ما يبررها من أسباب ثلاثة: الأول هو أن كل نظام من النظم الشهيرة المنتشرة يتميز فى عدة نواح، ويفتقر إلى نواح أخرى. وليست هذه هي كل المشكلة، فالميزة التي يتميز بها نظام قد تستفيد منها جهة ما، ولا تستفيد منها جهة أخرى، ذلك لأن لكل جهة ظروفها وحجم شبكتها ومستوى الخبراء والفنيين فيها. والعكس صحيح كذلك، فقد تكون هناك ثغرة خطيرة، أو نقطة ضعف فى أحد النظم، ولكنها لا تؤثر في بعض الجهات، التي قد يكون لديها برامج أو أجهزة تسد هذه الثغرة، أو تتجاوز نقطة الضعف هذه.

أما السبب الثاني فهو أن كلاً من هذه النظم يصدر نسخة جديدة كل عام أو عامين، ولذلك فالمقارنة تتوقف بشكل كبير على النسخة التى نأخذها فى الاعتبار وقت المقارنة. فقد تظهر المقارنة تفوقًا لنظام معين، ولكن تأتى النسخة الجديدة من النظام الآخر لتتفوق على نظيرتها فى هذا النظام فتقلب الموازين. لذلك فمن المهم عند التقييم أن نحدد نسخة نظام التشغيل التى نبنى عليها هذا التقييم.

السبب الثالث هو أن هذه النظم لم تعد الآن مجرد نظام تشغيل بسيط. بل تعقدت وأصبحت بيئات عمل كاملة، فى كل منها نظام تشغيل، ونظم مصاحبة، وأدوات برمجية، وتسهيلات مختلفة تقدمها الشركات. ولذلك فماذا نقارن؟ وماذا نقيم؟ هل نقيم نظام التشغيل وحده؟ أم نقيم ما يصاحبه من برمجيات؟ بعض هذه البرمجيات قد يكون ملازمًا لنظام التشغيل ويأتى معه باستمرار وبعضها اختياري، قد تفضل المؤسسة شراءه أو تحجم عن شرائه. وقد تفضل بعض المؤسسات شراء البرمجيات المصاحبة من طرف ثالث (Third Party)، ويحدث هذا كثيرًا مع بيئة التشغيل " يونكس ". فهل نقيم هذه البرمجيات التى يقدمها الطرف الثالث أيضًا باعتبارها جزءًا من نظام التشغيل؟

ولقد غامرنا في الفصل التاسع من هذا الكتاب (جدران الحماية) بمقارنة بيئات التشغيل، وتحدثنا عن أيها أنسب لتركيب جدران الحماية، وقد خلصنا من هذه المقارنة بنصيحة قدمناها لمسئول أمن المعلومات بأن يستخدم (كبيئة لجدار الحماية) نظام

التشغيل الذي يعرف عنه الكثير، ويتمكن من التعامل معه بكفاءة بغض النظر عن العوامل الأخرى.

على أية حال لن يمنعنا ذلك من إلقاء الضوء على بعض النقاط الأمنية الهامة في كل من نظم التشغيل الشهيرة (أو قل بيئات التشغيل)، ليس بهدف تفضيل أحدها على الآخر ولكن بهدف لفت نظر مسئول الأمن إلى معلومات قد يهمه معرفتها.

برغم هذه الصعوبات جميعها، إلا أن كتابة هذا الفصل كانت على جانب من السهولة، حيث وجدت أنني لست فى حاجة إلى شرح الكثير من المصطلحات الفنية أو التقنيات الحديثة أو الأجهزة والنظم التي تحدثنا عنها وشرحنا استخداماتها في فصول الكتاب الأحد عشر السابقة، فذكرتها دون شرح مع الإشارة، كلما وجدت ذلك ضرورياً، إلى الفصل الذي تم الحديث عنها فيه، حتى يستطيع القارئ الكريم الرجوع إلى هذه المعلومات إن شاء.

١٢ ـ ١ الأمن فى نظام " نتوير " (NetWare):

حديثنا عن نظام " نتوير " (NetWare) سيكون بالدرجة الأولى عن نسخة النظام رقم (٥,٠). وهذا النظام حائز على شهادة مستوى (C٢) لأمن الشبكات من " مركز أمن الحاسبات القومى " (NCSC) بالولايات المتحدة (انظر الملحق رقم (١) في نهاية الكتاب عن مستويات الأمن في نظم الحاسب)، وكذلك على شهادة مستوى (E٢) من المركز المناظر في أوربا. وهذه الشهادات، وإن كانت لا تضمن للمؤسسة نظاماً غير قابل للاختراق، إلا أنها تؤكد أن هذا النظام قد تم تصميمه مع الأخذ في الاعتبار كل الاحتياطات الأمنية التي تشترطها هذه الشهادات.

١٢ ـ ١ ـ ١ صلاحيات استخدام الملفات:

يستخدم نظام " نتوير " أسلوب " إدارة صلاحيات الاستخدام " (NDS) أو

(NetWare Directory Services) لتحديد صلاحيات استخدام الشبكة، مما يمكن من إدارة الشبكة بأكملها من خلال جهاز مراقبة واحد (Console) ويمكن من خلال هذا النظام تفويض بعض الصلاحيات لمساعدين لمدير الشبكة، أو لمديري الشبكات الفرعية، كل فيما يخص شبكته. ويمكن لهذا النظام التعامل مع الحالات الخاصة التى يظهر فيها التداخل بين احتياجات المستفيدين.

١٢ ـ ١ ـ ٢ حسابات المستفيدين:

يمكن التعامل مع حسابات المستفيدين مباشرة من خلال الخادم، فيمكن تحديد الصلاحية الأمنية للمستفيد من خلال التسهيلات التالية:

(١) **تسجيل معلومات المستفيد:** كالاسم والموقع والإدارة التى يعمل بها ورقم الهاتف...إلخ.

(٢) **قيود الدخول:** مثل تحديد تاريخ معين لانتهاء صلاحية حساب هذا المستفيد، أو تحديد الخوادم التي يمكنه الدخول إليها. وهذا جيد من الناحية الأمنية، إذ يكشف حالات انتحال الشخصية، إذا اكتشف المستفيد أنه لا يستطيع الدخول بسبب وجود شخص آخر بنفس الاسم يعمل على الشبكة في نفس الوقت وهكذا يمكن ألا يسمح الخادم بدخول نفس المستفيد أكثر من مرة في الوقت الواحد.

(٣) **قيود كلمة السر:** وتستخدم لتحديد قيود معينة على كلمة السر المسموح بها، كأن يفرض على المستفيد تغيير كلمة السر من آن لآخر، أو تحديد حد أدنى لحروف كلمة السر، أو تحديد عدد محاولات الدخول الفاشلة قبل قيام النظام بإغلاق الحساب.

(٤) **قيود توقيت الدخول:** تتيح هذه الإمكانية تحديد أوقات معينة لدخول المستفيدين، كأن يتم منع دخولهم إلى النظام خارج أوقات الدوام الرسمي، أو في عطلات نهاية الأسبوع. ويمكن تنفيذ ذلك بصورة منفردة لكل مستفيد. وتفيد هذه الإمكانية في إخراج المستفيدين من الشبكة عند بدء إعداد النسخة الاحتياطية، لضمان عدم وجود ملفات مفتوحة فى ذلك الوقت مما يعوق إعداد النسخة الاحتياطية.

(٥) **قيود عنوان الشبكة:** تتيح هذه الإمكانية تحديد الأجهزة المسموح للمستفيد بتعريف نفسه من خلالها. ويفيد ذلك في منع المستفيدين من الدخول بأسمائهم من أجهزة أخرى، ويمنع ذلك، إلى حد كبير، عمليات انتحال الشخصية.

(٦) **حجب المقتحمين:** من خلال هذه الإمكانية يمكن لمدير النظام مراقبة عدد محاولات الدخول الفاشلة، والتأكد من أن النظام قد حجب الحساب الذي حاول الدخول عدة مرات بكلمة سر خاطئة. ويمكن الاستفادة من هذه الإمكانية في حجب الموقع الذي دخل منه المقتحم بالكامل، كما يمكن الاستفادة منها عند ملاحقة المجرم، كما بينا في الفصل السابق.

(٧) **صلاحيات استخدام الملفات:** يمكن من خلال هذه الإمكانية مراجعة كل الصلاحيات الممنوحة لمستفيد معين على كافة الملفات، ويتفوق نظام " نتوير " في هذه الناحية على نظام " وندوز إن تي " مثلاً، الذي يحتاج فيه المسئول إلى مراجعة الملفات (أو الفهارس) واحداً واحداً لمعرفة صلاحيات المستفيد عليها. وسنبين عند حديثنا عن نظام " وندوز إن تي " كيف عالج نظام " الدليل النشط " هذه الثغرة. وإن كانت هناك ثغرة في نظام " نتوير " تتطلب انتباه مدير الشبكة، وهي صلاحية منح حق الاستخدام (Access Control Right) وهي إذا منحت لشخص ما، وليكن المستفيد (أ)، على فهرس معين فإنه يستطيع منح حقوق القراءة والكتابة ومنح حق الاستخدام لشخص آخر، وليكن المستفيد (ب)، على هذا الفهرس، حتى لو لم تكن هذه الحقوق لدى المانح (أ) نفسه . وبعد ذلك يمكن للشخص الذي حصل على هذه الحقوق (ب) أن يمنح بدوره حقوق القراءة والكتابة للشخص الأول (أ). وبذلك يتم التحايل وحصول (أ) على حقوق لم تكن ممنوحة له من قبل.

(٨) **مجموعات المستفيدين:** يمكن ضم أي مستفيد لمجموعة معينة فيحصل بذلك على كافة الصلاحيات الممنوحة لهذه المجموعة، وذلك بهدف تسهيل منح الصلاحيات.

(٩) **نسخ الصلاحيات:** من أجل تسهيل عملية منح الصلاحيات يمكن استخدام إمكانية نسخ الصلاحيات من شخص لآخر، كما يمكن بواسطة هذه الإمكانية قيام

مدير الشبكة بالمراقبة والتأكد من أن أحداً لم يحصل بطريقة ما على صلاحيات مكافئة لمدير الشبكة مثلاً.

١٢-١-٣ تأمين الاتصالات عبر الشبكة:

يقوم نظام التشغيل " نتوير " بتأمين الاتصالات مع خادم الشبكة عن طريق استخدام " بصمة الحزمة " (Packet Signature) وهى الوسيلة التي تواجه أحد أساليب انتهاك الشبكات التى تحدثنا عنها في الفصل الخامس، وهى أسلوب اختطاف الموقع (Site Hijacking)، حيث يقوم المقتحم بالاستيلاء على جلسة اتصال يقوم بها مدير الشبكة بعد أن ينتهي هذا المدير من تعريف نفسه لخادم الشبكة. فيضع المقتحم نفسه في الوسط بين المدير وخادم الشبكة، ويقوم بتزوير ما شاء من بيانات. وتتطلب وسيلة " بصمة الحزمة " من كل من الخادم ومحطة العمل (التي يعمل عليها مدير الشبكة) تعريف نفسيهما بشكل مستمر، ومع كل حزمة رسالة متبادلة بينهما، باستخدام مفتاح سرى يتم تبادله عند بداية الجلسة. وقد شرحنا استخدام هذه الوسيلة فى الفصل السابع. وهذه البصمة تتغير باستمرار وبشكل آلى من حزمة إلى أخرى.

كما توجد إمكانية إتاحة هذه الوسيلة " بصمة الحزمة " لجميع المستفيدين على الشبكة، ولو أن ذلك سيؤثر على الأداء الكلى للشبكة. كما توجد فى نظام " نتوير " إمكانية قيام مدير الشبكة بعملية تصفية الحزم باستخدام برنامج (Filtcfg)، حيث يمكّن خادم الشبكة من القيام بمهمة " مصفاة الحزم الاستاتيكية " التي شرحنا مهمتها في الفصل التاسع. وبذلك يمكن التحكم فى الرسائل المارة من وإلى خادم الشبكة، كما يمكن كذلك التحكم في الرسائل المارة إلى أجزاء أخرى من الشبكة (وذلك بتركيب عدد إضافي من بطاقات الشبكة في خادم الشبكة الرئيسي).

١٢ ـ ١ ـ ٤ أدوات إضافية لمدير الشبكة:

يمكن لمدير الشبكة تحسين مستوى الأمن فى النظام باستخدام بعض الوسائل الإضافية المتاحة له مثل:

(١) **برنامج (Secure.ncf)**: هذا البرنامج يمكن تشغيله آلياً عند بدء تشغيل خادم الشبكة، وهو يقوم بتنفيذ بعض العمليات الأمنية المفيدة مثل: عدم السماح بكلمات السر غير المشفرة، وعدم السماح للمستفيد العادي باستخدام أدوات المراقبة.

(٢) **أمر (Secure Console)**: عند إصدار هذا الأمر من خادم الشبكة يتم منع أي جهاز مرتبط بالشبكة (غير الخادم) من تحميل برامج النظام. وذلك بهدف منع أى مهاجم من إعادة تحميل هذه البرامج بعد أن يكون قد عبث بها، كما أنه يمنع تعديل الوقت والتاريخ إلا بواسطة مشغل الشبكة، ليمنع التلاعب في تحديد وقت إرسال أو استقبال البريد الإلكتروني مثلاً، أو استخدام الأجهزة في غير الأوقات المرخص بها.

(٣) **تأمين استخدام خادم الشبكة عن بعد:** يمكن لمدير الشبكة التعامل عن بعد مع جهاز مراقبة خادم الشبكة (Console)، وإصدار الأوامر له عن بعد. ويتم تشفير كلمة السر لتفادي قيام أحد المهاجمين بالتقاطها خلال تعامل مدير الشبكة مع الخادم عن بعد. وإن كانت هناك ثغرة فى هذا الأسلوب عندما يسمح بالتعامل مع جهاز مراقبة الخادم (Console) عن بعد باستخدام خدمة (Telnet)، حيث يتم ذلك باستخدام كلمة السر مفتوحة، لأن تشفيرها يكون قد تم فكه قبل ذلك. وهى من الثغرات التي تعرضنا لها، ولكيفية معالجتها من قبل.

١٢ ـ ٢ الأمن فى نظام " وندوز إن تي " (Windows NT):

حديثنا عن نظام " وندوز إن تي " (Windows NT) سيكون منصباً على النسخة ٤,٠ بالإضافة إلى النسخة التجريبية (Beta Version) من نظام النوافذ (NT ٥,٠) الخاصة بإدارة الشبكات الصادرة عام ٢٠٠٠ . هذه النسخة بصفة عامة تتميز بسهولة الاستخدام مقارنة بنظام التشغيل " نتوير "، وربما كان هذا راجعًا لشيوع

استخدام نظم النوافذ من " مايكروسوفت ". وشهدت هذه النسخة هجومًا كثيرًا مؤخرًا بسبب بعض الثغرات الأمنية التي استغلها المهاجمون في مهاجمة بعض المواقع التي تستخدم هذا النوع من نظم التشغيل. كما استغل مروجو الفيروسات ثغرة في أحد برامج هذه النسخة لترويج دودة الكمبيوتر التي اشتهرت باسم (Codered)، والتي ضربت أنحاء كثيرة من العالم في أغسطس ٢٠٠١م [Codered ٢٠٠٣]. الأمر نفسه حدث مع فيروس بلاستر الذي ضرب شبكات العالم في صيف عام ٢٠٠٣م. ولكن الحقيقة أن هذا النظام إذا تمت تهيئته بشكل جيد، فإن هذه الثغرات يمكن التغلب عليها. أما إذا تم تركيب نسخة النظام كما هي، بالقيم الافتراضية(default values) دون تغيير، فإن ذلك يجعله نظامًا ضعيفًا من الناحية الأمنية.

ويلاحظ أن نظام " وندوز إن تي " يفتقر إلى إمكانيات " نتوير " في التعامل عن بعد، وإن كان ذلك مما يسعد مسئولي أمن المعلومات لأنه يغلق بابًا واسعًا يأتي منه الريح.

يحقق النظام أسلوب عزل التطبيقات في ذاكرة خادم الشبكة (Memory isolation) وهو من الأمور الأساسية التي يشترطها الحصول على ترخيص مستوى (C٢) السابق الحديث عنه.

يهاجم الكثير من مؤيدي الخصوصية الفردية وجود ملف (Registry)الخاص بالنظام، والذي يضم معلومات كثيرة عن محتويات الجهاز، وعن صاحب الجهاز. وبرغم فوائد وجود هذا الملف إلا أن وصول المهاجم إلى البيانات التي يحتويها يهدد أمن الشبكة، لأن المهاجم إما أن يستفيد من هذه البيانات، أو يقوم بتخريب هذا الملف لحرمان خادم الشبكة من القدرة على الاستفادة من البرامج والتطبيقات المسجلة في هذا الملف، أو قد يتلاعب المهاجم بهذه البيانات فيغير من تهيئة خادم الشبكة.

١٢ـ٢ـ١ صلاحيات استخدام الملفات:

يستخدم النظام " هيكل النطاقات " (NT Domain Structure) لإدارة صلاحيات استخدام النظام. والنطاق (Domain) في هذه الحالة هو مجموعة من محطات العمل وأجهزة الخدمة تطبق سياسة أمنية مشتركة. ومن ثم فيستطيع المستفيد أن يدخل إلى

النظام مرة واحدة (بكلمة سر واحدة)، فيتاح له استخدام كامل أجهزة المجموعة (النطاق) .

ولكن يعيب هذا الأسلوب ما تعود عليه كثير من مسئولي الشبكات من أن يضعوا قواعد السياسة الأمنية في برنامج الدخول (Logon Script)، حتى يضمنوا تشغيله باستمرار عند دخول المستفيد إلى الجهاز. ولكن يستطيع المستفيد الذي يريد التهرب من الالتزام بهذه القواعد أن يضغط مفتاح (Ctrl + C)أثناء بدء التشغيل ليوقف تنفيذ قواعد السياسة الأمنية، ويستطيع بعد ذلك تشغيل أي برنامج يريد بدلاً منها.

ويستخدم نظام " ويندوز إن تي " في نسخ الصلاحيات أسلوب " منح الثقة بين النطاقات "(Domain Trusts)، مما يتيح للمستفيدين في نطاق ما الاحتفاظ بنفس مستوى صلاحياتهم في نطاق آخر، ولكن العكس غير صحيح . فإذا قلنا إن النطاق (أ) منح الثقة (trust) للنطاق (ب)، فإن ذلك يعني أن كل المستفيدين الذين لديهم صلاحيات ضمن النطاق (ب) (النطاق الموثوق به) يصبح لهم نفس الصلاحيات على موارد النطاق (أ) (النطاق مانح الثقة). ونظرًا لأن النطاق (ب) لم يمنح الثقة للنطاق (أ)، فإن العكس غير صحيح. أي أن مستفيدي النطاق (أ) لا يتمتعون بصلاحياتهم على النطاق (ب). وبرغم ذلك توجد إمكانية منح الثقة في اتجاهين أو " الثقة المتبادلة " (two-way trust). هذا الأسلوب قد يصلح للشبكات الصغيرة، أما في الشبكات الكبيرة فليس من العملي أن ينتقل مدير الشبكة إلى كل " نطاق " لتهيئته بشكل منفرد. كما أنه في حالة الرغبة في منح الصلاحية لعدد محدد من المستفيدين، يصعب تنفيذ ذلك من خلال منح الثقة من نطاق كامل لنطاق آخر كامل. ويتفوق نظام " نتوير " في هذه النقطة بالذات، حيث يمكن إنشاء (alias object) يضم المستفيدين المطلوب معاملتهم معاملة خاصة. كما أنه لا يمكن مراجعة كافة عمليات منح الثقة بين النطاقات من نقطة واحدة مركزية، وإنما يجب مراجعة كل خادم رئيسي في كل نطاق على حدة لاكتشاف علاقات منح الثقة بينه وبين النطاقات الأخرى. ويمكن لمسئول الشبكة المتمرس إعداد شبكة كاملة من " الثقة المتبادلة " ومستوياتها المختلفة لشبكة كبيرة.

١٢-٢-٢ حسابات المستفيدين:

يمكن إدارة حسابات المستفيدين فى نظام " وندوز إن تي " باستخدام برنامج " مدير النطاقات "(User Manager for Domains Utility)، والذي يسمح بإضافة مستفيدين جدد أو حذفهم، كما يسمح بتحديد مجموعات المستفيدين ، وتعريف سياسة الاستخدام. وهو يتولى إدارة كل ما يتعلق بصلاحيات المستفيدين ، إلا فيما يتعلق بصلاحيات استخدام الملفات والفهارس والسماح بالتشارك فيها، وهذه تتم من خلال " مستكشف نوافذ إن تى " (Windows NT Explorer). وتتم إدارة حسابات المستفيدين من خلال الإمكانيات التالية:

١٢-٢-٢-١ " المميز الأمني "(Security Identifier):

"المميز الأمنى " (SID) أو (Security Identifier) فى نظام التشغيل " وندوز إن تى " هو رقم فريد (غير متكرر) يميز كل مستفيد أو مجموعة من المستفيدين . ويشترك المستفيدون، والمجموعات التي تنتمي إلى نطاق معين، في الجزء الأول من هذا الرقم. أما الجزء الأخير منه والذي يسمى (Subauthority) فهو لا يتكرر، وبذلك فإن الرقم بالكامل يظل فريداً لكل مستفيد، ولكل مجموعة.

هذا الجزء الأخير (Subauthority) يشكل ثغرة أمنية، لأنه يكاد يكون معروفاً أو مشهوراً. فمثلاً في الحساب الخاص بمدير الشبكة (administrator) يأخذ هذا الجزء (Subauthority) القيمة (٥٠٠)، ومن ثم يستطيع المهاجم استنتاج " المميز الأمني " لمدير الشبكة في نطاق معين إذا حصل على المميز الأمني لأي مستفيد في هذا النطاق. في هذه الحالة يقوم المهاجم بحذف الجزء الأخير (Subauthority) ويضع بدلاً منه القيمة المعروفة لمدير الشبكة . وقد نشرت شركة مايكروسوفت في إحدى وثائقها (Microsoft Knowledgebase document Q١٦٣٨٤٦) قائمة بكل هذه المميزات الأمنية المشهورة مع أرقام الحسابات الخاصة بها!! [Brenton ١٩٩٩]. ولذا ننصح (وتنصح شركة مايكروسوفت) مدير الشبكة بضرورة تغيير اسم حساب مدير

الشبكة واستخدام كلمة سر صعبة.

وإن كان " ردني " في موقعه [Rudnyi ٢٠٠٣] قد أورد مجموعة من البرامج يمكن الحصول عليها من هذا الموقع، للحصول على أسماء حسابات مديري الشبكة! ويقوم أحد هذه البرامج (User ٢ sid) بتغيير الجزء الأخير من " المميز الأمني " (SID) لأي مستفيد أو مجموعة في النطاق، ويستبدل به الرقم (٥٠٠) مثلاً للحصول على " مميز أمني " له صلاحيات مدير الشبكة.

١٢ ـ ٢ ـ ٢ ـ ٢ " **مدير الحساب الأمني** "(Security Account Manager):

"مدير الحساب ا لأمني " (SAM) أو (Security Account Manager) هو ملف يتم فيه الاحتفاظ بكل بيانات المستفيدين كالاسم، والمميز الأمني، ونسخة مشفرة من كل كلمة سر استخدمها. وهذا الملف لا يمكن الوصول إليه من جانب المستفيد العادي.

ولكن هناك نسخ احتياطية من هذا الملف مخزنة في صورة مضغوطة، فإذا استطاع المهاجم الوصول إلى هذا الملف أو إلى نسخته الاحتياطية فإنه سيكون في مقدوره اختراق النظام.

١٢ ـ ٢ ـ ٢ ـ ٣ تحديد سياسة الصلاحيات:

يمكن تحديد سياسة الصلاحيات في نظام " وندوز إن تي " من خلال كل مما يأتي:

[١] حد أقصى لمدة صلاحية كلمة السر.

[٢] حد أدنى لمدة صلاحية كلمة السر، وذلك لمنع المستفيد من تغيير كلمة السر ثم محاولة العودة إلى كلمة السر القديمة مرة أخرى.

[٣] حد أدنى لعدد حروف كلمة السر.

[٤] عدم استخدام كلمات سر قديمة مرة أخرى.

[٥] حد أقصى لمحاولات الدخول الفاشلة التي يترتب عليها إغلاق الحساب، ويمكن تحديد فترة زمنية تحتسب خلالها هذه المحاولات (نصف ساعة مثلاً) يعود بعدها العداد إلى الصفر،ويسمح بمحاولة الدخول مرة أخرى. كما يمكن تحديد مدة معينة يغلق خلالها الحساب ثم يعاد فتحه مرة أخرى.

[٦] فصل المستفيدين آلياً في حالة انتهاء الفترة المسموح لهم فيها بالبقاء في النظام، ويمكن الاستفادة من ذلك في إغلاق الملفات قبل البدء في إعداد النسخ الاحتياطية للنظام.

[٧] يوجد إمكانية لفرض ضرورة دخول المستفيد إلى النظام بكلمة سر صحيحة قبل السماح له بتغيير كلمة السر، وذلك لمنع أي مهاجم من استغلال أي ثغرة في النظام لتغيير كلمة سر أحد المستفيدين واستخدام الكلمة الجديدة في الدخول بدلاً منه.

١٢-٢-٣ مراقبة الوقائع (Event Viewer):

يمكن تسجيل ومتابعة كل وقائع الاستخدام من خلال نظام " مراقبة الوقائع " (Event Viewer)، ويمكن لمدير النظام تحديد نوع الوقائع التي يتم تسجيلها، مما يتيح إمكانيات هائلة تسمح بتسجيل كل ما يدور من وقائع في النظام. ويفضل عند تهيئة هذا النظام عدم السماح بإعادة الكتابة على سجل الوقائع. كما يجب إفراغ هذا السجل أولاً بأول حفاظاً على توافر المعلومات لمدد طويلة سابقة (ستة أشهر مثلاً).

١٢-٢-٤ تصفية الحزم (Packet filtering):

يدعم نظام التشغيل " وندوز إن تي " أسلوب " تصفية الحزم "(Packet filtering) للرسائل المارة بخادم الشبكة. ولكنها تستخدم أسلوب التصفية الاستاتيكي مما لا يمكن من التمييز بين الرسائل السليمة والرسائل التي قد يقحمها المهاجم في النظام (انظر الفصل التاسع من الكتاب). ولكن النظام لا يقوم بتسجيل وجود أي تعارض بين

التطبيقات التي تعمل على منفذ معين في خادم الشبكة. يعني ذلك أن التسجيل لن يظهر في نظام مراقبة الوقائع رسالة الخطأ التي تبين المنافذ التي قد يتم إغلاقها بواسطة مصفاة الحزم، وذلك قد يتسبب في تضليل مدير النظام الذي يتابع نظام مراقبة الوقائع فيظن أن جميع التطبيقات والمنافذ تعمل بشكل منتظم على عكس الواقع.

١٢-٢-٥ " الدليل النشط " (Active Directory):

أعتقد أن " الدليل النشط " (Active Directory) من " شركة مايكروسوفت " يشكل جزءًا من منظومة كاملة صاحبت ظهور (الجيل الجديد) من " وندوز إن تي "، ولعل القارئ يلاحظ أنني استخدمت تعبير (الجيل الجديد) بدلاً من النسخة الجديدة، لأن " وندوز إن تي " الآن لم يعد مجرد نظام تشغيل فقط، بل مجموعة متكاملة من النظم. وقد حسَّن " الدليل النشط " إلى حد كبير من أسلوب " النطاقات "، كما حل العديد من المشكلات التي ذكرنا أنها كانت تعوق التعامل المنفرد مع مجموعات المستفيدين، وساعد استخدامه على زيادة اللامركزية في الخدمات الأمنية. ولذلك تروج مايكروسوفت لهذا " الدليل النشط " لما حققه من طفرة أمنية وساعد على انتشار منتجها(SQL Server) لكي تنافس به النظم القديمة المستقرة.

كما أن استخدام شركة " ميكروسوفت " لأسلوب " أداة المراقبة المركزية " (Microsoft Management Console) في النسخة الحديثة من النظام قد ساعد على إيجاد نقطة مركزية واحدة للتعامل مع كافة خوادم (NT) في الشبكة.

وتدعم النسخة الحديثة من النظام أسلوب (Kerberos) للتحقق من الشخصية الذي تحدثنا عنه من قبل في الفصل السابع، كما تتمتع هذه النسخة بميزة تتفوق فيها على نظام " نتوير " ونظام " يونكس "، وهي دعم الشهادات الرقمية، ودعم أسلوب المفتاح العلني، كما تدعم " البطاقات الذكية "(Smart cards).

١٢ـ٣ الأمن في نظام " يونكس " (UNIX):

على العكس من نظام " نتوير " ونظام " وندوز إن تي " فإن نظام التشغيل " يونكس " لا يتمتع بواجهة رسومية مريحة (GUI) أو (Graphical User Interface)، باستثناء بعض تطبيقات " لينكس " مثل (Red hat) ولذلك يجب على مدير النظام أن يكون متمرسًا في استخدام هذا النظام وأوامره، وإلا كانت المحافظة على أمن النظام عبئًا ثقيلاً ومهمة غير مضمونة.

وإذا كان مدير النظام يعرف كيف يستفيد من إمكانيات " يونكس " وتوظيفها أمنيًا فإنه بذلك سيكون لديه نظام تشغيل أكثر أمنًا من النظم الأخرى. فمثلاً خادم " إن تي " الذي يستخدم نظام " خادم معلومات الإنترنت " (IIS) أو (Internet Information Server) يتطلب أن يكون منفذ (RPC) وهو رقم (١٣٥)، وكل منافذ (NetBIOS) وهي من (١٣٧) إلى (١٣٩) تظل مفتوحة، لتظل جاهزة لاستقبال طلبات الخدمة من المستفيدين، ومن ثم معرضة للانتهاك أثناء التشغيل. ولكن نظام " يونكس " الذي يستخدم نظام " أباتشي " (Apache) لا يتطلب فتح المنافذ إلا حين تقديمها للخدمة فعلاً (مثل منفذ ٨٠ لخدمة الاتصال بالإنترنت) وهذا يضيق الثغرات المتاحة أمام المهاجمين.

١٢ـ٣ـ١ صلاحيات استخدام الملفات:

يستخدم نظام " يونكس " كلاً من " رمز المستفيد " (UID) أو (User ID)، و" رمز المجموعة " (GID) أو (Group ID) من أجل تعريف المستفيدين. وعند إنشاء مستفيد لأحد الملفات، فإن النظام يقوم بتخزين " رمز المستفيد " و" رمز المجموعة "، للمستفيد الذي قام بإنشاء الملف، مع الملف نفسه. وبذلك يصبح هذا المستفيد هو " مالك الملف " (File Owner).

ولكن ربما كان أسلوب تحديد صلاحيات استخدام الملفات هو إحدى الثغرات الأمنية الواضحة في نظام " يونكس ". فهذه الصلاحيات يتم منحها على ثلاثة مستويات

مختلفة: " المالك " (لمنشئ الملف)، و" المجموعة " (لمجموعة من المستفيدين)، و" الجميع " (لكل المستفيدين). وتقتصر الصلاحيات التي يمكن منحها على " القراءة "، و"الكتابة"، و" التنفيذ "فقط، ولا يستخدم نظام " يونكس " صلاحيات " التعديل "، أو "الحذف". وتنشأ عن هذا مشكلتان:

الأولى أنك قد تستطيع أن تمنع استخدام ملف ما من جانب " الجميع "، بأن تحدد صلاحية الاستخدام لتصبح (No access)، ولكن ذلك لن يمنع ظهور اسم الملف أمام الجميع. ومعرفة المهاجم بوجود هذا الملف سوف تدفعه إلى محاولة الحصول على الصلاحية اللازمة للوصول إليه.

والثانية أن الصلاحيات فضفاضة جدًا، فأنت لا تستطيع أن تمنح صلاحية "القراءة" على ملف معين لشخصين بعينهما مثلاً ضمن مجموعة معينة، على أن تكون لباقي أفراد هذه المجموعة صلاحية " الكتابة " على هذا الملف !

نجد أن الصلاحيات الافتراضية في معظم نظم " يونكس " متساهلة كثيرًا، لذلك فعلى مسئول الأمن مراجعة هذه الصلاحيات وتعديلها قبل السماح للمستفيدين بمزاولة أعمالهم.

من الثغرات الأمنية في استخدام صلاحيات الملفات، أن المستفيد يحتاج بالفعل إلى أن تكون لديه صلاحية " القراءة " على ملفات النظام حتى يستطيع أداء عمله. ولكن ذلك يسمح له بالتجول هنا وهناك، وفحص ما يشاء من الملفات. وربما قاده ذلك إلى العثور على ثغرة تمكنه من اقتناص صلاحيات أعلى مما يستحق.

١٢ ـ ٣ ـ ٢ حسابات المستفيدين:

يمكن إدارة حسابات المستفيدين على كل نظام من نظم " يونكس " بشكل منفصل، أو إدارة مجموعة من النظم التي تستخدم " يونكس " (أو أحد أنظمة عائلة " يونكس " مثل " لينكس " (Lynux)، وذلك مركزيًا عن طريق استخدام نظام " خدمات معلومات

الشبكة " (NIS) أو (Network Information Services)، وهو ملف يضم معلومات المستفيدين والمجموعات الأعضاء في أكثر من نظام من نظم " يونكس " لتتشارك هذه النظم في استخدام معلومات هذا الملف. وهذه النظم التي تضمها مجموعة واحدة وتتشارك في ملف " خدمات معلومات الشبكة " يطلق عليها اسم " النطاق "(Domain) ولكي نمنح المستفيد صلاحيات على " النطاق " يتم إضافة هذا المستفيد إلى ملف (NIS) المخزن على الخادم الرئيسي للمجموعة، وعند رغبة المستفيد في استخدام نظام معين يقع ضمن " النطاق " فإن هذا النظام سوف يراجع ملف (NIS) الرئيسي للتأكد من صلاحية هذا المستفيد للدخول. أي أن المستفيد يستطيع الدخول إلى نظام ما دون أن يكون مسجلاً أصلاً على هذا النظام.

وفي هذا الصدد نجد أن نظام " يونكس " في استخدامه للنطاقات ليس أفضل حالاً من " وندوز إن تي " في نسختها الرابعة، التي تستخدم النطاقات أيضًا (قبل ظهور " الدليل النشط "). فالمستفيد الذي يمنح صلاحية على نطاق (NIS) يستطيع استخدام أي نظام داخل النطاق كله ولا توجد وسيلة لمنعه من استخدام نظام معين بالذات داخل هذا النطاق، وإذا كان ذلك ضروريًا فيجب إعادة توزيع النطاقات وتوزيع النظم على هذه النطاقات.

١٢-٣-٢-١ ملف كلمات السر:

يتم التحقق من شخصية المستفيدين باستخدام ملف كلمات السر الذي يضم اسم المستفيد وكلمة السر (المشفرة)، ورمز المستفيد (UID)، ورمز المجموعة (GID)، وغير ذلك من المعلومات. وتمنح صلاحيات كاملة للمستفيد الرئيسي (root)، والذي يحصل عليه عادة مديرالنظام. ويتميز نظام " يونكس " هنا بأن بعض الخدمات كثيرة الاستخدام، مثل خدمة (FTP) وخدمة (Telnet) وغيرها تستخدم رمزًا معينًا للمستفيد وللمجموعة يختلف عن رمز المستفيد والمجموعة للمستفيد ذي الصلاحيات الكاملة (root)، ومن ثم فإذا تمكن المهاجم من اختراق إحدى هذه الخدمات، فإنه لا يكون لديه

الصلاحيات الكاملة التي يمنحها رمز (root) ويلجأ نظام " يونكس " إلى وضع رمز (*) مكان كلمة السر للحسابات المغلقة لمنع أصحابها من الدخول إلى النظام.

هناك مشكلة أمنية أخرى تتعلق بملف كلمات السر، وهي ضرورة حصول جميع المستفيدين على صلاحية القراءة على هذا الملف ليمكنهم إثبات شخصيتهم، ولكن أحد حقول هذا الملف يضم كلمة السر المشفرة كما أسلفنا. هنا يمكن لأي مستفيد أن يحصل على نسخة من ملف كلمات السر، ويحاول على جهاز منفصل كسر كلمات السر باستخدام أسلوب المحاولة والخطأ. ويواجه نظام " يونكس " هذه الثغرة الخطيرة مواجهة حاسمة بأن يستخدم خوارزمية تشفير قوية للغاية لتشفير كلمات السر، وهي خوارزمية (DES) ذات ٥٦ خانة [1] حيث يكون " النص الصريح " المدخل للخوارزمية هو مجموعة من الأصفار، ويكون مفتاح التشفير هو كلمة السر المدخلة من المستفيد. ويتم تكرار تشفير " النص المشفر " المخرج من الخوارزمية عدة مرات بالدخول في نفس الحلقة ٢٥ مرة. ولزيادة تعقيد عملية التشفير يستخدم مفتاح ثان يعتمد على توقيت إدخال كلمة السر (Time of day)، وهو يتراوح بين الصفر و (٤,٠٩٥). ويضمن ذلك أنه إذا أدخل اثنان من المستفيدين نفس كلمة السر فإن " النص المشفر " لن يكون هو نفسه في الحالتين. هذا المفتاح الإضافي يسمى " حبة الملح " (Salt grain)، وهي ما تعطي المذاق الطيب للطعام عند طهيه. وحتى يمكن فك شفرة النص المشفر فإن هذا المفتاح الجديد (وهو مكون من حرفين) تتم إضافته إلى النص المشفر. وعند التحقق من شخصية المستفيد، يتم فصل هذين الحرفين عن النص المشفر واستخدامهما في تشفير كلمة السر المدخلة من المستفيد ثم مطابقة النص المشفر الناتج مع النص المخزن في ملف كلمات السر.

يتضح من ذلك مناعة أسلوب التشفير المتبع، فكيف إذًا يستطيع المهاجم كسر كلمة

---

[1] للحصول على معلومات عن كيفية عمل هذه الخوارزمية يمكن الرجوع إلى كتاب "الحاسب وأمن المعلومات" من منشورات معهد الإدارة العامة – ٢٠٠٠م.

السر؟ إنه لا يستطيع فك التشفير بعملية عكسية لأنه سيحصل عندئذٍ على النص الصريح، وهو مجرد مجموعة من الأصفار. المهاجم في هذه الحالة يفعل ما يفعله النظام عند التحقق من شخصية المستفيد، فيفصل المهاجم الحرفين (حبة الملح) من النص المشفر، ثم يحاول تشفير مجموعة الأصفار باستخدام كلمات سر عديدة (عن طريق التجربة والخطأ)، مع استخدام " حبة الملح " التي حصل عليها، إلى أن يصل إلى الكلمة التي تتطابق مع " النص المشفر ". ويمكنه لتحقيق ذلك استخدام قاموس اللغة الإنجليزية (أو غيرها). ولذلك ينصح بالابتعاد عن استخدام مثل هذه الكلمات عند اختيار كلمة السر، وينصح باستخدام الأرقام ضمن حروف كلمة السر، وينصح كذلك باستخدام الحروف الصغيرة (Lower case) والحروف الكبيرة (Upper case) معاً.

تلجأ بعض نظم " يونكس " إلى استخدام ملف " الظل " لكلمات السر المشفرة أو (Shadow passwords)الذي لا يستطيع الاطلاع عليه سوى مدير النظام (Root) فقط. في هذه الحالة يحتوي ملف كلمات السر الأصلي في حقل كلمة السر المشفرة على الحرف (X)، مما يعني للنظام أن عليه البحث عن كلمة السر المشفرة في ملف " الظل ".

١٢-٣-٢-٢ ملف المجموعات:

يعتمد نظام " يونكس "، كما أسلفنا، على " رمز المستفيد " و" رمز المجموعة ". ومن ثم فالنظام يحتفظ بملف " المجموعات " الذي يضم " رمز المجموعة " والمستفيدين الأعضاء في هذه المجموعة. فإذا أنشأ مستفيد ضمن مجموعة ما ملفاً فإن كل أعضاء المجموعة يصبح لهم حق " المالك " في استخدام هذا الملف، وهذا ينتج ثغرة أمنية حقيقية.

وللتغلب على ذلك فإن المستفيدين الآخرين ضمن المجموعة يمنحون فقط حق " القراءة " للملفات التي يقوم زملاؤهم في المجموعة بإنشائها. وفي حالة الحاجة إلى منحهم صلاحيات أكثر، فإن ذلك يتم من خلال أوامر منح الصلاحية.

ملحق رقم (١)
مستويات الأمن في نظم الحاسب

نشرت وزارة الدفاع الأمريكية الكتاب البرتقالي عن تصنيف أمن نظم الحاسب الآلي والمسمى : "Trusted Computer System Evaluation Criteria" .[DoD ٢٠٠٣] ورغم أن هذا التصنيف كان مقصوداً به في البداية تصنيف النظم العسكرية إلا أنه الآن أصبح واسع الاستخدام في صناعة الحاسب الآلي. ويتراوح هذا التصنيف من الفئة "د" (D) وهي الفئة التي تمثل أدنى مستوى من مستويات الحماية إلى الفئة " أ "(A) التي تمثل أعلى مستويات الحماية. وهي على النحو التالي :

(١) الفئة " د "(D) أدنى مستويات الحماية:

وتقع في هذه الفئة النظم التي لا ينطبق عليها أيٌ من تصنيفات الفئات الأخرى، أو تلك التي لا تتمتع بالخصائص الأمنية التي تؤهلها لاحتلال مرتبة أعلى في التصنيف، وعمليًا لا توجد نظم كثيرة واقعة في هذه الفئة.

(٢) الفئة " جـ " (C) الحماية الاختيارية:

يقع في هذه الفئة مستويان من مستويات الحماية الاختيارية هما المستوى " جـ ١ " (C١) ثم المستوى الأعلى " جـ ٢ (C٢).

[١] مستوى الحماية الأمنية الاختيارية " جـ ١ " (C١)، ويتميز بكل مما يأتي:

- وجود قوائم للسماح بالاستخدام للمستفيدين مع تقسيم المستفيدين إلى مجموعات متشابهة الصلاحيات.
- عادة يعامل المستفيدون في هذا المستوى على نفس المستوى الأمني.
- وجود قاعدة بيانات لتحديد صلاحيات المستفيدين.
- حماية أمنية لنظام التشغيل وبرامجه.

- إجراء اختبارات دورية.
- اختبار الآليات الأمنية المستخدمة مع عدم السماح بالالتفاف حولها.
- توثيق كل من أمن المستفيدين وأمن مسئولي النظام إلى جانب توثيق الاختبارات التي تجري على النظام.

ولا يقع الكثير من النظم في هذه الفئة، ومن أمثلة النظم الواقعة فيها: النسخ الأولى من نظام " يونكس " (UNIX) ونظام الحماية والسرية " راكف " (RACF) من شركة " ا ب م " (IBM).

[٢] مستوى الحماية " جـ٢ " (C٢)، ويتميز بكل ما يتميز به المستوى " جـ ١ " (C١)بالإضافة إلى ما يلي:

- إمكان تطبيق الحماية لكل مستفيد على حدة (عن طريق قوائم تحديد الصلاحيات).
- لا يتم منح صلاحيات الاستخدام إلا من خلال المستفيدين المخولين بذلك.
- وجود إجراءات يتم فرض تنفيذها لتحديد شخصية المستفيد والتحقق منها، مثل رقم المستفيد وكلمة السر.
- رقابة كاملة على كافة وقائع الاستخدام مع تسجيل الواقعة وتاريخها ووقتها والمستفيد الذي قام بها ونجاحها أو فشلها والطرفية التي تم الدخول منها.
- حماية إضافية للبيانات ومتابعة تعديلها وتوثيق هذه التعديلات.

ويقع في هذه الفئة معظم النظم المعروفة مثل نظام التشغيل (VMS)، ونظام (OS/٤٠٠) من شركة " ا ب م "، ونظام " وندوز إن تي "، و" نتوير ٤,١١ " من شركة نوفيل، ونظام قواعد البيانات " أوراكل ٧ ".

(٣) الفئة " ب " (B) للحماية الإجبارية:

الحماية في هذه الفئة إجبارية وليست اختيارية. وتقع فيها ثلاثة مستويات تبدأ

بالمستوى " ب ١ " (B١) ثم تصعد للمستوى " ب ٢ " (B٢) ثم تصعد لأعلى مستوى في هذه الفئة وهو المستوى " ب ٣ " (B٣) وهي على النحو التالي :

[١] مستوى الحماية الأمنية الإجبارية " ب ١ " (B١)

ويشمل هذا المستوى كل ما يشمله المستوى " جـ ٢ " (C٢) بالإضافة إلى ما يلي:

- فرض الحماية الإجبارية وتحديد صلاحيات استخدام كل من الملفات والإجراءات والأجهزة ... إلخ.
- التأكد من صحة وتكامل البيانات عند تداولها، ومراقبة عمليات التداول رقابة كاملة.
- فرض التأكد من صلاحيات الاستخدام عند التعامل مع جميع موارد الحاسب.
- طباعة تقارير مقروءة عن الحالة الأمنية، أو إخراجها على شاشة مثلاً.
- تحسين مستوى التوثيق ومستوى حماية نظام التشغيل.

ومن أمثلة النظم الواقعة في هذه الفئة نظام (SEVMS) من شركة " ديجيتال "، ونظام (CS/SX) من شركة " هاريس ".

[٢] مستوى الحماية الأمنية الهيكلية " ب ٢ "(B٢)

ويشمل هذا المستوى كل ما يشمله المستوى " ب ١ "(B١) بالإضافة إلى ما يلي :

- القدرة على اكتشاف أي تغيير يطرأ على مستوى الأمن مما يؤثر على المستفيد الذي يقوم بالاتصال المباشر (Interactive user).
- وجود مسار اتصال آمن بين المستفيد والنظام.
- أمن تنفيذ أوامر التشغيل في هذا المستوى أكثر إحكامًا.
- وجود اختيارات أمنية أفضل.

ومن أمثلة النظم الواقعة في هذه الفئة نظام (VSLAN) من شركة " كريبتك ".

[٣] مستوى النطاقات الأمنية " ب ٣ "(B٣)

ويشمل هذا المستوى كل ما يشمله المستوى " ب ٢ " (B٢) بالإضافة إلى ما يلي:

- تعتمد قوائم الاستخدام في نفس الوقت على كل من المجموعات ورموز الاستخدام.
- وجود تحليل أمني تلقائي بشكل مستمر.
- التأكد من فاعلية الرقابة على الوقائع الأمنية.
- توفر استعادة آمنة للوضع عقب انهيار النظام مع توثيق كامل لكافة الوقائع المرتبطة بالانهيار.
- عدم وجود أي ثغرات أمنية في تصميم النظام وأدنى حد من الثغرات الأمنية عند التطبيق.

وربما كان نظام التشغيل الوحيد الذي وصل إلى هذه الفئة العالية هو نظام التشغيل (XTS-٣٠٠) من شركة " جترونكس/وانج ".

(٤) الفئة " أ " (A) للحماية المؤكدة:

هذه الفئة هي أعلى الفئات الأمنية للنظم وتتضمن المستوى " أ ١ "(A١) ثم يتدرج بعد ذلك إلى مستويات أعلى مثل " أ ٢ " (A٢) وأعلى من ذلك.

[١] مستوى الحماية المؤكدة " أ ١ "(A١)

ويشمل هذا المستوى كل ما يشتمل عليه المستوى " ب ٣ " (B٣) بالإضافة إلى :

- وجود أساليب للتأكد من سلامة قواعد الحاسب المؤمنة (TCB)

ولا يوجد في هذا المستوى سوى نظام (MLS LAN) من شركة " بوينج "، ونظام (Gemini Trusted Network Processor)، ونظام (SCOMP) من شركة " هني ويل ".

[٢] مستويات الحماية المؤكدة " أ ٢ " (A٢) وما بعدها

تم اعتبار المستويات الأمنية الأعلى من " أ ١ " برغم أنه حتى الآن لا توجد نظم تم تصنيفها في فئات أعلى من " أ ١ "(A١)

المراجع

Abrams, Marshall D. & Podell, Harold J.: "Malicious Software". Book chapter of "Information Security an integrated collection of essays" Essay ٤ p.p. ١١١ Edited by Abrams, Marshall D. Jajodia, Sushil & Podell, Harold J. IEEE Computer Society Press California U.S.A. ١٩٩٨.

ADSL: "http://www.adsl.com/adsl_tutorial.html", accessed on ٢/١١/ ٢٠٠٣.

Baker, McBride & Coles: "http://www.mbc.com/ecommerce/ecom_overview.asp", accessed on ٢٠ August ٢٠٠٣.

Bentley, Tom R.: "Safe Computing", Untechnical press, CA., USA, ٢٠٠٠.

Bower, Dan M.: "Access Control & Personal Identification Systems" Butterworths ١٩٩٦.

Brenton, Chris: "Mastering Network Security", SyBEX, Network Press, USA, ١٩٩٩.

Burns, Tim: "Entrepreneurship.com", Dearborn, USA, ٢٠٠١.

Code red: "http://www.macafee.com/anti-virus/viruses/codered/default.asp", accessed on ٧ Dec. ٢٠٠٣.

Denning, D.: "The Clipper Encryption System", American Scientist, July-August ١٩٩٣ pp. ٣١٩-٣٢٣.

Ditlea, S.: "The PC goes Ready-to-Wear" IEEE spectrum, October ٢٠٠٠, pp. ٣٤:٣٩.

DoD, "The Orange book summary", Department of Defence: "http://www.dynamoo.com/orange/summary.htm", accessed on ١ Dec. ٢٠٠٣.

Elliot, J.: "Distributed denial of service attacks and the Zombie ant effect", IEEE ITPro, ٢(٢), March/ April ٢٠٠٠ p.p. ٥٥-٥٧.

Erbschloe, Michael and John Vacca: "Net Privacy: a guide to developing and implementing an ironclad e business privacy plan", McGraw-Hill, ٢٠٠١.

Escamilla, Terry: "Intrusion Detection: Network security beyond the fire-wall", Wiley, ١٩٩٨.

Garfinkel, Simson & Gene Spafford: "Practical UNIX & Internet Security" ٢nd ed., Sebastopol, CA: Oreilly & Associates, ١٩٩٦.

Ghosh, A. K.: "Code-driven attacks: the evolving internet threat", proceedings of the information survivability workshop ٢٠٠٠, Boston, MA., USA, October ٢٤-٢٦, ٢٠٠٠.

Ghosh, Anup K.: "Security & privacy for e-business", John Wiley, USA, ٢٠٠١.

GSMDATA: "http://www.gsmdata.com", accessed on ٢٠ Nov ٢٠٠٣.

Halfhill, T.R.: "Cheaper Computing", BYTE magazine, April ١٩٩٧, pp.٦٦-٨٠.

Halsall, Fred: "Data Communications, Computer Networks and Open Systems", ٤th ed., Addison-Wesley, ١٩٩٦.

Hamilton, S.: "E-Commerce for the ٢١st century", IEEE Computer Vol. ٣٠, No.٥, May ١٩٩٧, pp. ٤٤-٤٧.

Hyatt, Michael S.: "Invasion of privacy: how to protect yourself in the digital age", Regnery publishing, USA, ٢٠٠١.

Icove, David, Karl Seger & William VonStorch: "Computer Crime: A crime fighter's Handbook", O'Reilly & Associates, ١٩٩٥.

Internetsizer: "http://www.netsizer.com", accessed on ١/٨/٢٠٠٣.

Kaeo, Merike: "Designing Network Security: a practical guide to creating a secure network infrastructure", Cisco press, Macmillan technical publishing, USA, ١٩٩٩.

Kagan, Richard S.: "Virtual Private Networks - New strategies for Secure Enterprise Networking", IEEE, ١٩٩٨, pp. ٢٦٧-٢٧٢.

Kambil, A.: "Doing Business in the Wired World", IEEE Computer Vol.٣٠, No.٥, May ١٩٩٧, pp:٥٦-٦١.

Loshin, Pete "TCP/IP clearly explained", second edition, AP Professional, USA, ١٩٩٧.

McClure, Stuart, Joel Scambray & George Kurtz: "Hacking Exposed: Network security secrets and solutions", Osborne, McGraw-Hill, ١٩٩٩.

McGraw, Gary & Ed Felten: "Java security: Hostile applets, holes, and

antidotes", John Wiley, USA, ١٩٩٦.

McGraw, Gary & Greg Morriset: "Attacking malicious code: a report to the infosec research council", Submitted to IEEE software and presented to the IRC, USA, May ٢٠٠٠.

Microsoft: "Microsoft Virtual Private Networking: Using point-to-point tunneling protocol for low-cost, secure, remote access across the Internet", white paper, pre-release, ٢٨/٠٥/٢٠٠٠.

Nachenberg, Carey: "Virus protection techniques" , ACM communications journal, ١٩٩٧.

Naval Surface Warfare Center Dahlgren Division: "http://www.nswc.navy.mil", accessed ٢٨ Nov ٢٠٠٣.

Northcutt, Stephen: "Network Intrusion Detection: an analyst's handbook", New Riders Publishing, USA, ١٩٩٩.

Nua: [http://www.nua.net/surveys/how-many-online/index.html], accessed on ٢١ JAN. ٢٠٠٣.

Ogletree, Terry William: "Practical Firewalls", Que, USA, ٢٠٠٠.

Parker, Donn B.: "Fighting computer crime", John Wiley, USA, ١٩٩٨.

Pfleeger, Charles P.: "Security in Computers" ٢nd edition, Prentice Hall, ١٩٩٧.

Purdue:"http://ww.cs.purdue.edu/coast/intrusion-detectiondetection.html", accessed on ١٢ Oct. ٢٠٠٣.

Reynolds, Janice: "The complete e-commerce book: Design, Build & maintain a successful web-based business", CMP Books, New York, ٢٠٠٠.

Rudnyi, Evgenii: "http://www.ntbugtraq.com", accessed on ٢٠ Oct. ٢٠٠٣.

Symantec: "Symantec security updates home page: top threats", http://www.symantec.com/avcenter/. Accessed on ١٥/٨/٢٠٠٣.

Telcordia: "http://www.telcordia.com", accessed on ١٠/١٠/٢٠٠٣.

Tripwire: "http://tripwiresecurity.com", accessed on ١١ Nov. ٢٠٠٣.

Vinet, R.: "Business-to-Business E. Commerce to lead the way", E. Commerce Today, Vol. ٩٦.١١.٢٩ November ٢٩, ١٩٩٦.

WAPFORUM: "http://www.wapforum.com", accessed on ٢ Dec ٢٠٠٣.

Zalewski, Michal: "I don't think I really love you: writing internet worms for fun and profit", report of 'Samhain' project, http://lcamtuf.na.export.pl/worm.txt, ٢٠٠٠.

Zwicky, Elizabeth D., Simon Cooper & D. Brent Chapman: "Building Internet Firewalls", ٢nd ed., OREILLY, USA, ٢٠٠٠.

داود، حسن طاهر: " الأمن في عصر المعلومات "، أكاديمية نايف العربية للعلوم الأمنية، الرياض، تحت الطبع، ٢٠٠٤م.

داود، حسن طاهر: " الحاسب وأمن المعلومات "، معهد الإدارة العامة، الرياض، ٢٠٠٠م.

داود، حسن طاهر: " جرائم نظم المعلومات "، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٠م.

غنيمي، محمد أديب رياض: " مستقبل الحاسبات "، المكتبة الأكاديمية، كراسات علمية، ٢٠٠١م.

معجم عربى / إنجليزى

Proxy	أجهزة التفويض " بروكسي "
Hosts	أجهزة الحاسب المستضيفة
Clients	أجهزة الموظفين (العملاء)
Firewall appliances	أجهزة جدران الحماية
Scanners	أجهزة فحص الشبكات
Intrusion detection products, Intrusion Detectors	أجهزة كشف الاقتحام
Multiple-purpose boxes	أجهزة متعددة الاستخدام
Mail forwarding	إحالة الرسائل
Configuration errors	أخطاء التهيئة
Console	أداة المراقبة
Microsoft Management Console	أداة المراقبة المركزية لمايكروسوفت
Packet analyzer	أداة تحليل الحزم
NetWare Directory Services (NDS)	إدارة صلاحيات الاستخدام من " نتوير "
Spam mail	إرسال البريد الإلكتروني لآلاف المستفيدين
Sequence numbers	أرقام التسلسل
Acknowledgment numbers	أرقام التعارف
Dial-up access	أسلوب الاتصال المراقم
Tunneling	أسلوب النفق في الاتصال
Gigabit-capacity point of presence (Gigapops)	أسلوب نقاط التجميع
Terrestrial microwave	أشعة الميكروويف الأرضية
Dishes	أطباق الاستقبال
Replay	إعادة إرسال الرسائل

Reboot	إعادة تشغيل الجهاز
Buffer overflow	إغراق مساحات الذاكرة الوسيطة بالبيانات
Graceful shutdown	إغلاق الأجهزة بشكل نظامي
Data injection & modification	إقحام المعلومات وتعديلها
Subversion	إقحام نسخة أخرى من البرنامج
Silent alarm	إنذار صامت
Subpatterns	أنماط فرعية
System shutdown	إنهاء النظام
Site Hijacking	اختطاف المواقع
Caching	استخدام الذاكرة الخبيئة
Single-box architecture	استخدام جهاز واحد
Domain Name	اسم النطاق
Session hijacking	اعتراض البث
Octopus	الأخطبوط
Digital Envelopes	الأغلفة الرقمية
Satellites	الأقمار الاصطناعية
Engine	الآلة
Optical fiber	الألياف الضوئية
False positive	الإنذار الكاذب بالاقتحام
Object Database Connectivity (ODBC)	الاتصال الشيئي بقواعد البيانات
remote access	الاستخدام عن بعد
Unauthorized access	الاستخدام غير المرخص به
Back door	الباب الخلفي

Troubleshooting	البحث عن حل المشكلة
Utilities	البرامج المساعدة
Browsers	البرامج المستعرضة
Malicious code	البرامج ذات الأهداف الشريرة
Privileged Programs	البرامج ذات الصلاحيات العالية
Object-oriented programming	البرمجة الشيئية
Email	البريد الإلكتروني
Smart cards	البطاقات الذكية
e-banking	البنك الإلكتروني
Electronic banking	البنوك الإلكترونية
Public Key Infrastructure (PKI)	البنية الأساسية للمفتاح العلني
Electronic Commerce	التجارة الإلكترونية
Dense Wavelength Division Multiplexing (DWDM)	التجميع المبني على التقسيم الموجي المكثف
Roaming	التجوال
Authentication	التحقق من الشخصية
Overloading	التحميل الزائد
Crosstalk	التداخل
Web?based training	التدريب عن طريق الإنترنت
Authorization	الترخيص بالاستخدام
Encryption	التشفير
Symmetric cryptography	التشفير المتماثل
Public key cryptography	التشفير باستخدام المفتاح العلني
Asymmetric cryptography	التشفير غير المتماثل

Computer aided design	التصميم باستخدام الحاسب
Collision	التضارب
Distance learning	التعليم عن بعد
Spoofing	التنصت
Routing	التوجيه
Time of day	التوقيت
Digital signatures	التوقيعات الرقمية
two-way trust	الثقة المتبادلة
Trust	الثقة في المعلومات
Virtual universities	الجامعات الافتراضية
Mobile Computer	الحاسب المتنقل
Portable Computer	الحاسب المحمول
Super computers	الحاسبات العملاقة
Lower case	الحروف الصغيرة
Upper case	الحروف الكبيرة
Distributed computing	الحساب الموزع
Online Virtual Reality	الحقيقة الافتراضية المباشرة
Electronic Government	الحكومة الإلكترونية
Pretty Good Privacy (PGP)	الخصوصية الفائقة
Privacy and Confidentiality	الخصوصية وسرية المعلومات
Shielded Twisted Pair (STP)	الخطوط المزدوجة المجدولة المعزولة
Unshielded Twisted Pair (UTP)	الخطوط المزدوجة المجدولة غير المعزولة
Two-wire open lines	الخطوط المزدوجة المفتوحة

Application Specific Integrated Circuit (ASIC)	الدائرة المتكاملة المخصصة للتطبيق
Active Directory	الدليل النشط
Worms Against Nuclear Killers (WANK)	الدودة النووية
Vampire worm	الدودة مصاصة الدماء
Cache memory	الذاكرة الخبيئة
Security association	الربط الآمن
Message digests	الرسائل المركزة
Master boot record	السجل الرئيسي لبدء التشغيل
Optical fiber networks	الشبكات الضوئية
Independent screened subnets	الشبكات الفرعية المحجوبة المستقلة
Wide Area Networks	الشبكات الكبيرة
Dedicated WANs	الشبكات الكبيرة الخاصة
Local area networks	الشبكات المحلية
Trans-European Network	الشبكة الأوروبية
Perimeter network	الشبكة الخارجية
Virtual Private Network (VPN)	الشبكة الخاصة الافتراضية
Synchronous Optical Network (SONET)	الشبكة الضوئية المتزامنة
Subnet	الشبكة الفرعية
Screened subnet architecture	الشبكة الفرعية المحجوبة
Split-screened subnet	الشبكة الفرعية المحجوبة المقسمة
LAN	الشبكة المحلية
Noise	الشوشرة
Home pages	الصفحات الخاصة

Telemedicine	الطب عن بعد
٣-D Holography	العرض الهولوجرافي ثلاثي الأبعاد
Backbone	العمود الفقري
Hardware address, Media Access Control (MAC)	العنوان المادي
Virus	الفيروس
Companion virus	الفيروس المصاحب
Polymorphic virus	الفيروس متعدد الأوجه
e-mail lists	القوائم البريدية الإلكترونية
Default values	القيم الافتراضية
Hash	القيمة الاختبارية
Cables	الكابلات
Coaxial cables	الكابلات المحورية
Checksum	المجموع الاختباري
Switches	المحولات
Optical Switches	المحولات الضوئية
Medium Earth Orbit (MEO)	المدار الأرضي المتوسط
Low Earth Orbit (LEO)	المدار الأرضي المنخفض
Geosynchronous Earth Orbit (GEO)	المدار المتزامن مع الأرض
Null	المساحات الخالية في الملف
Mobile user	المستخدم المتنقل
Optical receiver	المستقبل الضوئي
Parallel processing	المعالجة المتوازية
Public key	المفتاح العلني

Security Identifier (SID)	المميز الأمنى
Ports	المنافذ
Demilitarized zone (DMZ)	المنطقة الوسيطة
Hacker	المهاجم أو المقتحم
Exterior router	الموجه الخارجي
Interior router	الموجه الداخلي
Snapshot	النسخة الاحتياطية اللحظية
Beta Version	النسخة التجريبية للبرامج
Open systems	النظم المفتوحة
Secured tunnel	النفق الأمن
Wireless ATM	النقل اللاسلكي غير المتزامن
Duplex transmission	النقل في اتجاهين
Point to point	النقل من نقطة محددة إلى نقطة أخرى
Enterprise Security Model	النموذج الأمني للمؤسسة
Antennas	الهوائيات
Virtual reality	الواقع الافتراضي
Impersonation	انتحال الشخصية
r-utilities	برامج ((rالمساعدة
Active X controls	برامج " أكتف إكس "
Java attack applets	برامج " جافا " الهجومية
Web browsers	برامج استعراض الإنترنت
Attack scripts	برامج الهجوم
CPU-bound	برامج تعتمد بشدة على قدرات المعالج

Password crackers	برامج كسر كلمات السر
Mobile code	برامج منقولة
User Manager for Domains Utility	برنامج إدارة النطاقات
Internet explorer	برنامج التصفح
Routine	برنامج صغير لمهمة محددة
Source code	برنامج في صورة المصدر
Cryptographic Checksumming Program	برنامج مشفر للمجموع الاختباري
Internet Protocol (IP)	بروتوكول الإنترنت
Mobile Internet Protocol	بروتوكول الإنترنت المتنقل
Transmission Control Protocol/ Internet Protocol (TCP/IP)	بروتوكول التحكم في النقل/ بروتوكول الإنترنت
Wireless Application Protocol (WAP)	بروتوكول التطبيقات اللاسلكية
Address Resolution Protocol (ARP)	بروتوكول ترجمة العناوين
User Datagram Protocol (UDP)	بروتوكول حزم المستخدم
Internet Control Message Protocol (ICMP)	بروتوكول متابعة الرسائل
Intrusion signatures	بصمات الاقتحام
Signature	بصمة
Time stamp	بصمة التوقيت
Packet Signature	بصمة الحزمة
Encryption cards	بطاقات التشفير
Network card	بطاقة الشبكة
I-banking	بنوك الإنترنت
Three?tier structure	بنية الطبقات الثلاث
Gateway	بوابة

Application-level gateway	بوابة التطبيقات
Timeout error	تجاوز الفترة الزمنية
Identification and authentication	تحديد الشخصية والتحقق منها
Ping of Death	تخريب النظام
Photo transistor	ترانزيستور الصورة
Network Address Translation (NAT)	ترجمة عناوين الشبكة
Logging, Accounting	تسجيل وقائع الاستخدام
System startup	تشغيل النظام
Site Browsing	تصفح المواقع
Packet filtering	تصفية الحزم
Firewall design	تصميم جدران الحماية
Modulation	تعديل الإشارة
Data mining	تعدين البيانات
Vulnerability assessment	تقييم درجة ضعف النظام
Firewall implementation	تنفيذ جدران الحماية
Hang	توقف الجهاز عن العمل
Signature	توقيع
Firewall	جدار الحماية
Routing table	جدول التوجيه
State table	جدول الحالة
Love bug	جرثومة الحب
Communication session	جلسة اتصال
Pass phrase	جملة المرور

Alta Vista tunnel	جهاز " نفق ألتافسيتا "
Radio transmitter	جهاز إرسال
Network analyzer	جهاز تحليل الشبكة
Notebook	جهاز حاسب دفتري
Onetime password hardware	جهاز لاستخدام كلمة السر لمرة واحدة
Monitor	جهاز مراقبة
Dual-homed host	جهاز مزدوج الاتصال
Network Computer	حاسب الشبكة
Bastion host	حاسب منيع
Salt grain	حبة الملح
Packets, Datagrams	حزم الرسائل
Guest account	حساب ضيف
Hidden accounts	حسابات المستفيدين المخفاة
Trojan horse	حصان طروادة
Flag field	حقل العلامات
Length Field	حقل طول الرسالة
Fragmentation offset field	حقل مؤشر التجزئة
Cluster computing	حوسبة المجموعات
Web server	خادم الإنترنت
Proxy server	خادم البروكسي
FTP proxy server	خادم البروكسي المتخصص في نقل الملفات
e-mail server	خادم البريد الإلكتروني
Encryption server	خادم التشفير

Network access server	خادم الشبكة
Screened host architecture	خادم الشبكة المحجوب
Print server	خادم الطباعة
Internet Information Server (IIS)	خادم معلومات الإنترنت
FTP server	خادم نقل الملفات
Network Information Services (NIS)	خدمات معلومات الشبكة
Domain Name Service (DNS)	خدمة أسماء النطاق
Remote Address Dial-In User Service (RADIUS)	خدمة الاتصال عن بعد " راديوس "
Telnet service	خدمة الدخول عن بعد
United States Postal Service (USPS)	خدمة بريد الولايات المتحدة
Simple Mail Transport Protocol (SMTP)	خدمة نقل البريد
File Transfer Protocol (FTP)	خدمة نقل الملفات
Trivial FTP (TFTP)	خدمة نقل الملفات البسيطة
Asymmetric Digital Subscriber Line (ADSL)	خط المشترك الرقمي غير المتماثل
Dial-up lines	خطوط المراقمة
Leased lines	خطوط خاصة مستاجرة
Data links	خطوط نقل البيانات
Mail servers	خوادم البريد
Hash algorithm	خوارزمية القيمة الاختبارية
Transponder	دائرة النقل
Great internet worm	دودة الإنترنت الهائلة
Worm	دودة الحاسب
IRC worm	دودة المحادثة

Build number	رقم التركيب
Group ID (GID)	رمز المجموعة
Personal Identification Number (PIN), User ID (UID)	رمز المستفيد
User ID (UID)	رمز المستفيد
Connection-establishment timer	زمن إتمام الاتصال
Traffic log	سجل الوقائع للرسائل المارة بالشبكة
System logs	سجلات وقائع استخدام النظام
Bandwidth	سعة الموجة
Certification authorities	سلطات منح الشهادات الرقمية
Public?key certification authorities	سلطات منح شهادات تعريف المفتاح العلني
Broadband networks	شبكات النطاق العريض
Extranet	شبكة إكسترانت
Intranet	شبكة الإنترانت
Integrated Services Digital Network (ISDN)	شبكة الخدمات الرقمية المتكاملة
World Wide Web	شبكة النسيج العالمية
Router-based network	شبكة تعتمد على الموجه
Firewall-based network	شبكة تعتمد على جدار الحماية
Network Of Workstations (NOW)	شبكة محطات العمل
Coarse beam	شعاع غير مركز
Fluctuating beam	شعاع متردد
Finely focused beam	شعاع مركز بشدة
Microwave beam	شعاع ميكروويف
Digital certificates	شهادات التعريف الرقمية

Server certificates	شهادات الخوادم
Data Integrity	صحة وسلامة البيانات
Web pages	صفحات الإنترنت
Access control	صلاحيات الاستخدام
Root privileges	صلاحيات عالية
Administrator-level authorities	صلاحيات مطلقة
Access Control Right	صلاحية منح حق الاستخدام
Executable code	صورة البرنامج القابلة للتنفيذ
Compression	ضغط
File compression	ضغط الملفات
Secure Socket Layer (SSL)	طبقة المدخل الآمنة
Skin effect	ظاهرة سريان التيار في المحيط الخارجي للسلك
False negative	عدم الإنذار في حالة الاقتحام
Denial of Service (DoS)	عرقلة الخدمة
Memory isolation	عزل التطبيقات في ذاكرة خادم الشبكة
Nodes	عقد
TCP flags	علامات حزم TCP
Eavesdropping	عمليات التنصت
Multiplexing	عملية التجميع/التوزيع
IP addresses	عناوين الإنترنت
Source IP address	عنوان الحاسب المرسل
Destination IP address	عنوان الحاسب المستقبل
IP subnet address	عنوان الشبكة الفرعية

Source and destination IP address	عنوان مصدر الرسالة وعنوان مستقبلها
Optical cladding	غلاف ضوئي
Application-level virus scanner	فاحص فيروسات التطبيقات
Virus scanners	فاحصات الفيروسات
Remote scanners	فاحصات عن بعد
Local scanners	فاحصات محلية
Decryption	فك الشفرة
Melissa virus	فيروس " ميليسا "
Cavity virus	فيروس الفجوة
Access Control List (ACL)	قائمة التحكم في الاستخدام
Base station	قاعدة
Knowledge-base	قاعدة المعرفة
Boot disk	قرص تشغيل
CD ROM	قرص مضغوط
Diode	قطب ثنائي
Light?Emitting Diode (LED)	قطب ثنائي باعث للضوء
Light-sensitive photodiode	قطب صورة ثنائي حساس للضوء
Laser Diode (LD)	قطب ليزر ثنائي
Duplex channel	قناة اتصال ذات اتجاهين
Communication links	قنوات الاتصال
Business rules	قواعد العمل
Intrusion detection and monitoring	كشف الاقتحام والمراقبة
Java script	لغة " جافا للنصوص "

Extended Markup Language (XML)	لغة العلامات الممتدة
File Owner	مالك الملف
Cluster Computers	مجموعات الحاسبات
Multiple screened subnets	مجموعة من الشبكات الفرعية المحجوبة
Search engines	محركات البحث
Very Small Aperture Terminals (VSAT)	محطات استقبال صغيرة
SMTP relay	محول البريد الإلكتروني
Band of frequencies	مدى معين من الترددات
Security Account Manager (SAM)	مدير الحساب الأمني
System Administrator, Supervisor	مدير النظام
Access Control	مراقبة الاستخدام
Packet sniffing	مراقبة الرسائل
Event Viewer	مراقبة الوقائع
Optical transmitter	مرسل ضوئي
Memory buffers	مساحات الذاكرة الوسيطة
Concurrent users	مستخدمو الشبكة في نفس الوقت
Anonymous user	مستفيد مجهول
Host-based	مستوى الحاسب المضيف
Network-based	مستوى الشبكة
Partnerships for Advanced Computational Infrastructure (PACI)	مشروع " المشاركة في البنية الأساسية للحوسبة
Packet filters	المتقدمة "
Static packet filter	مصافي الحزم
Dynamic packet filter	مصفاة الحزم الاستاتيكية

Processor	مصفاة الحزم الديناميكية
CPU usage	معالج
Routing information	معدل استخدام وحدة المعالجة المركزية
Service provider	معلومات توجيه الرسالة
Authentication Header (AH)	مقدم الخدمة
Header, IP Header	مقدمة التحقق من الشخصية
Shadow passwords file	مقدمة الرسالة
Registry	ملف " الظل " لكلمات السر المشفرة
Domain Trusts	ملف تسجيل البرامج
Boot sector	منح الثقة بين النطاقات
Data-driven attack	منطقة بدء التشغيل
Command-channel attack	مهاجمة البيانات
Radio waves	مهاجمة الخادم باستخدام الأوامر
Screening router	موجات الراديو
Encryption domain	موجه حاجب
Bluetooth	نطاق التشفير
Digital Encryption Standard (DES)	نظام " السن الزرقاء "
Triple DES	نظام التشفير الرقمي
Expert system	نظام التشفير الرقمي الثلاثي
Computer Misuse Detection System	نظام خبير
(CMDS)	نظام كشف سوء استخدام الحاسب
Public key encryption systems	نظم التشفير التي تستخدم المفتاح العلني
Extensible systems	نظم قابلة للتوسع

Intrusion Detection Systems (IDS)	نظم كشف الاقتحام
VPN tunnel	نفق الشبكة الخاصة الافتراضية
Teardrop attack	هجوم " قطرة الدمع "
Script kiddies	هواة استخدام برامج الاقتحام
NT Domain Structure	هيكل النطاقات لنظام وندوز إن تي
Graphical User Interface (GUI)	واجهة رسومية
Demultiplexers	وحدات إعادة التوزيع
Multiplexers	وحدات التجميع
Large key algorithm	وسائل تشفير ذات مفتاح طويل
Twisted pair access to the information highway	وسيلة الوصول إلى طريق المعلومات السريع عن طريق خطوط الهاتف

معجم إنجليزى / عربى

-D Holography۳	العرض الهولوجرافي ثلاثي الأبعاد
Access Control Right	صلاحية منح حق الاستخدام
Access control	صلاحيات الاستخدام
Access Control	مراقبة الاستخدام
Access Control List (ACL)	قائمة التحكم في الاستخدام
Acknowledgment numbers	أرقام التعارف
Active Directory	الدليل النشط
Active X controls	برامج " أكتف إكس "
Address Resolution Protocol (ARP)	بروتوكول ترجمة العناوين
Administrator-level authorities	صلاحيات مطلقة
Alta Vista tunnel	جهاز " نفق ألتافسيتا "
Anonymous user	مستفيد مجهول
Antennas	الهوائيات
Application Specific Integrated Circuit (ASIC)	الدائرة المتكاملة المخصصة للتطبيق
Application-level gateway	بوابة التطبيقات
Application-level virus scanner	فاحص فيروسات التطبيقات
Asymmetric cryptography	التشفير غير المتماثل
Asymmetric Digital Subscriber Line (ADSL)	خط المشترك الرقمي غير المتماثل
Attack scripts	برامج الهجوم
Authentication	التحقق من الشخصية
Authentication Header (AH)	مقدمة التحقق من الشخصية
Authorization	الترخيص بالاستخدام

Back door	الباب الخلفي
Backbone	العمود الفقري
Band of frequencies	مدى معين من الترددات
Bandwidth	سعة الموجة
Base station	قاعدة
Bastion host	حاسب منيع
Beta Version	النسخة التجريبية للبرامج
Bluetooth	نظام " السن الزرقاء "
Boot disk	قرص تشغيل
Boot sector	منطقة بدء التشغيل
Broadband networks	شبكات النطاق العريض
Browsers	البرامج المستعرضة
Buffer overflow	إغراق مساحات الذاكرة الوسيطة بالبيانات
Build number	رقم التركيب
Business rules	قواعد العمل
Cables	الكابلات
Cache memory	الذاكرة الخبيئة
Caching	استخدام الذاكرة الخبيئة
Cavity virus	فيروس الفجوة
CD ROM	قرص مضغوط
Certification authorities	سلطات منح الشهادات الرقمية
Checksum	المجموع الاختباري
Clients	أجهزة الموظفين (العملاء)

Cluster Computers	مجموعات الحاسبات
Cluster computing	حوسبة المجموعات
Coarse beam	شعاع غير مركز
Coaxial cables	الكابلات المحورية
Collision	التضارب
Command-channel attack	مهاجمة الخادم باستخدام الأوامر
Communication links	قنوات الاتصال
Communication session	جلسة اتصال
Companion virus	الفيروس المصاحب
Compression	ضغط
Computer aided design	التصميم باستخدام الحاسب
Computer Misuse Detection System (CMDS)	نظام كشف سوء استخدام الحاسب
Concurrent users	مستخدمو الشبكة في نفس الوقت
Configuration errors	أخطاء التهيئة
Connection-establishment timer	زمن إتمام الاتصال
Console	أداة المراقبة
CPU usage	معدل استخدام وحدة المعالجة المركزية
CPU-bound	برامج تعتمد بشدة على قدرات المعالج
Crosstalk	التداخل
Cryptographic Checksumming Program	برنامج مشفر للمجموع الاختباري
Data Integrity	صحة وسلامة البيانات
Data mining	تعدين البيانات
Data injection & modification	إقحام المعلومات وتعديلها

Data links	خطوط نقل البيانات
Data-driven attack	مهاجمة البيانات
Decryption	فك الشفرة
Dedicated WANs	الشبكات الكبيرة الخاصة
Default values	القيم الافتراضية
Demilitarized zone (DMZ)	المنطقة الوسيطة
Demultiplexers	وحدات إعادة التوزيع
Denial of Service (DoS)	عرقلة الخدمة
Dense Wavelength Division Multiplexing (DWDM)	التجميع المبني على التقسيم الموجي المكثف
Destination IP address	عنوان الحاسب المستقبل
Dial-up lines	خطوط المراقمة
Dial-up access	أسلوب الاتصال المراقم
Digital certificates	شهادات التعريف الرقمية
Digital Encryption Standard (DES)	نظام التشفير الرقمي
Digital Envelopes	الأغلفة الرقمية
Digital signatures	التوقيعات الرقمية
Diode	قطب ثنائي
Dishes	أطباق الاستقبال
Distance learning	التعليم عن بعد
Distributed computing	الحساب الموزع
Domain Name	اسم النطاق
Domain Trusts	منح الثقة بين النطاقات
Domain Name Service (DNS)	خدمة أسماء النطاق

Dual-homed host	جهاز مزدوج الاتصال
Duplex channel	قناة اتصال ذات اتجاهين
Duplex transmission	النقل في اتجاهين
Dynamic packet filter	مصفاة الحزم الديناميكية
Eavesdropping	عمليات التنصت
e-banking	البنك الإلكتروني
Electronic banking	البنوك الإلكترونية
Electronic Commerce	التجارة الإلكترونية
Electronic Government	الحكومة الإلكترونية
Email	البريد الإلكتروني
e-mail lists	القوائم البريدية الإلكترونية
e-mail server	خادم البريد الإلكتروني
Encryption	التشفير
Encryption cards	بطاقات التشفير
Encryption domain	نطاق التشفير
Encryption server	خادم التشفير
Engine	الآلة
Enterprise Security Model	النموذج الأمني للمؤسسة
Event Viewer	مراقبة الوقائع
Executable code	صورة البرنامج القابلة للتنفيذ
Expert system	نظام خبير
Extended Markup Language (XML)	لغة العلامات الممتدة
Extensible systems	نظم قابلة للتوسع

Exterior router	الموجه الخارجي
Extranet	شبكة إكسترانت
False negative	عدم الإنذار في حالة الاقتحام
False positive	الإنذار الكاذب بالاقتحام
File compression	ضغط الملفات
File Owner	مالك الملف
File Transfer Protocol (FTP)	خدمة نقل الملفات
Finely focused beam	شعاع مركز بشدة
Firewall	جدار الحماية
Firewall design	تصميم جدران الحماية
Firewall implementation	تنفيذ جدران الحماية
Firewall appliances	أجهزة جدران الحماية
Firewall-based network	شبكة تعتمد على جدار الحماية
Flag field	حقل العلامات
Fluctuating beam	شعاع متردد
Fragmentation offset field	حقل مؤشر التجزئة
FTP proxy server	خادم البروكسي المتخصص في نقل الملفات
FTP server	خادم نقل الملفات
Gateway	بوابة
Geosynchronous Earth Orbit (GEO)	المدار المتزامن مع الأرض
Gigabit-capacity point of presence (Gigapops)	أسلوب نقاط التجميع
Graceful shutdown	إغلاق الأجهزة بشكل نظامي
Graphical User Interface (GUI)	واجهة رسومية

Great internet worm	دودة الإنترنت الهائلة
Group ID (GID)	رمز المجموعة
Guest account	حساب ضيف
Hacker	المهاجم أو المقتحم
Hang	توقف الجهاز عن العمل
Hardware address, Media Access Control (MAC)	العنوان المادي
Hash	القيمة الاختبارية
Hash algorithm	خوارزمية القيمة الاختبارية
Header, IP Header	مقدمة الرسالة
Hidden accounts	حسابات المستفيدين المخفاة
Home pages	الصفحات الخاصة
Host-based	مستوى الحاسب المضيف
Hosts	أجهزة الحاسب المستضيفة
I-banking	بنوك الإنترنت
Identification and authentication	تحديد الشخصية والتحقق منها
Impersonation	انتحال الشخصية
Independent screened subnets	الشبكات الفرعية المحجوبة المستقلة
Integrated Services Digital Network (ISDN)	شبكة الخدمات الرقمية المتكاملة
Interior router	الموجه الداخلي
Internet Control Message Protocol (ICMP)	بروتوكول متابعة الرسائل
Internet explorer	برنامج التصفح
Internet Information Server (IIS)	خادم معلومات الإنترنت
Internet Protocol (IP)	بروتوكول الإنترنت

Intranet	شبكة الإنترانت
Intrusion detection and monitoring	كشف الاقتحام والمراقبة
Intrusion detection products, Intrusion Detectors	أجهزة كشف الاقتحام
Intrusion Detection Systems (IDS)	نظم كشف الاقتحام
Intrusion signatures	بصمات الاقتحام
IP subnet address	عنوان الشبكة الفرعية
IP addresses	عناوين الإنترنت
IRC worm	دودة المحادثة
Java attack applets	برامج " جافا " الهجومية
Java script	لغة " جافا للنصوص "
Knowledge-base	قاعدة المعرفة
LAN	الشبكة المحلية
Large key algorithm	وسائل تشفير ذات مفتاح طويل
Laser Diode (LD)	قطب ليزر ثنائي
Leased lines	خطوط خاصة مستأجرة
Length Field	حقل طول الرسالة
Light?Emitting Diode (LED)	قطب ثنائي باعث للضوء
Light-sensitive photodiode	قطب صورة ثنائي حساس للضوء
Local area networks	الشبكات المحلية
Local scanners	فاحصات محلية
Logging, Accounting	تسجيل وقائع الاستخدام
Love bug	جرثومة الحب
Low Earth Orbit (LEO)	المدار الأرضي المنخفض

Lower case	الحروف الصغيرة
Mail forwarding	إحالة الرسائل
Mail servers	خوادم البريد
Malicious code	البرامج ذات الأهداف الشريرة
Master boot record	السجل الرئيسي لبدء التشغيل
Medium Earth Orbit (MEO)	المدار الأرضي المتوسط
Melissa virus	فيروس " ميليسا "
Memory buffers	مساحات الذاكرة الوسيطة
Memory isolation	عزل التطبيقات في ذاكرة خادم الشبكة
Message digests	الرسائل المركزة
Microsoft Management Console	أداة المراقبة المركزية لمايكروسوفت
Microwave beam	شعاع ميكروويف
Mobile code	برامج منقولة
Mobile Computer	الحاسب المتنقل
Mobile Internet Protocol	بروتوكول الإنترنت المتنقل
Mobile user	المستخدم المتنقل
Modulation	تعديل الإشارة
Monitor	جهاز مراقبة
Multiple screened subnets	مجموعة من الشبكات الفرعية المحجوبة
Multiple-purpose boxes	أجهزة متعددة الاستخدام
Multiplexers	وحدات التجميع
Multiplexing	عملية التجميع/التوزيع
NetWare Directory Services (NDS)	إدارة صلاحيات الاستخدام من " نتوير "

Network access server	خادم الشبكة
Network Address Translation (NAT)	ترجمة عناوين الشبكة
Network analyzer	جهاز تحليل الشبكة
Network card	بطاقة الشبكة
Network Computer	حاسب الشبكة
Network Information Services (NIS)	خدمات معلومات الشبكة
Network Of Workstations (NOW)	شبكة محطات العمل
Network-based	مستوى الشبكة
Nodes	عقد
Noise	الشوشرة
Notebook	جهاز حاسب دفتري
NT Domain Structure	هيكل النطاقات لنظام وندوز إن تي
Null	المساحات الخالية في الملف
Object Database Connectivity (ODBC)	الاتصال الشيئي بقواعد البيانات
Object-oriented programming	البرمجة الشيئية
Octopus	الأخطبوط
Onetime password hardware	جهاز لاستخدام كلمة السر لمرة واحدة
Online Virtual Reality	الحقيقة الافتراضية المباشرة
Open systems	النظم المفتوحة
Optical receiver	المستقبل الضوئي
Optical cladding	غلاف ضوئي
Optical fiber	الألياف الضوئية
Optical fiber networks	الشبكات الضوئية

Optical Switches	المحولات الضوئية
Optical transmitter	مرسل ضوئي
Overloading	التحميل الزائد
Packet Signature	بصمة الحزمة
Packet analyzer	أداة تحليل الحزم
Packet filtering	تصفية الحزم
Packet filters	مصافي الحزم
Packet sniffing	مراقبة الرسائل
Packets, Datagrams	حزم الرسائل
Parallel processing	المعالجة المتوازية
Partnerships for Advanced Computational Infrastructure (PACI)	مشروع " المشاركة في البنية الأساسية للحوسبة المتقدمة "
Pass phrase	جملة المرور
Password crackers	برامج كسر كلمات السر
Perimeter network	الشبكة الخارجية
Personal Identification Number (PIN), User ID (UID)	رمز المستفيد
Photo transistor	ترانزيستور الصورة
Ping of Death	تخريب النظام
Point to point	النقل من نقطة محددة إلى نقطة أخرى
Polymorphic virus	الفيروس متعدد الأوجه
Portable Computer	الحاسب المحمول
Ports	المنافذ
Pretty Good Privacy (PGP)	الخصوصية الفائقة
Print server	خادم الطباعة

Privacy and Confidentiality	الخصوصية وسرية المعلومات
Privileged Programs	البرامج ذات الصلاحيات العالية
Processor	معالج
Proxy	أجهزة التفويض " بروكسي "
Proxy server	خادم البروكسي
Public key	المفتاح العلني
Public key cryptography	التشفير باستخدام المفتاح العلني
Public key encryption systems	نظم التشفير التي تستخدم المفتاح العلني
Public Key Infrastructure (PKI)	البنية الأساسية للمفتاح العلني
Public?key certification authorities	سلطات منح شهادات تعريف المفتاح العلني
Radio waves	موجات الراديو
Radio transmitter	جهاز إرسال
Reboot	إعادة تشغيل الجهاز
Registry	ملف تسجيل البرامج
remote access	الاستخدام عن بعد
Remote Address Dial-In User Service (RADIUS)	خدمة الاتصال عن بعد " راديوس "
Remote scanners	فاحصات عن بعد
Replay	إعادة إرسال الرسائل
Roaming	التجوال
Root privileges	صلاحيات عالية
Router-based network	شبكة تعتمد على الموجه
Routine	برنامج صغير لمهمة محددة
Routing	التوجيه

Routing information	معلومات توجيه الرسالة
Routing table	جدول التوجيه
r-utilities	برامج ((rالمساعدة
Salt grain	حبة الملح
Satellites	الأقمار الاصطناعية
Scanners	أجهزة فحص الشبكات
Screened host architecture	خادم الشبكة المحجوب
Screened subnet architecture	الشبكة الفرعية المحجوبة
Screening router	موجه حاجب
Script kiddies	هواة استخدام برامج الاقتحام
Search engines	محركات البحث
Secure Socket Layer (SSL)	طبقة المدخل الآمنة
Secured tunnel	النفق الآمن
Security Identifier (SID)	المميز الأمنى
Security Account Manager (SAM)	مدير الحساب الأمني
Security association	الربط الآمن
Sequence numbers	أرقام التسلسل
Server certificates	شهادات الخوادم
Service provider	مقدم الخدمة
Session hijacking	اعتراض البث
Shadow passwords file	ملف " الظل " لكلمات السر المشفرة
Shielded Twisted Pair (STP)	الخطوط المزدوجة المجدولة المعزولة
Signature	بصمة

Signature	توقيع
Silent alarm	إنذار صامت
Simple Mail Transport Protocol	خدمة نقل البريد
(SMTP)	استخدام جهاز واحد
Single-box architecture	تصفح المواقع
Site Browsing	اختطاف المواقع
Site Hijacking	ظاهرة سريان التيار في المحيط الخارجي للسلك
Skin effect	البطاقات الذكية
Smart cards	محول البريد الإلكتروني
SMTP relay	النسخة الاحتياطية اللحظية
Snapshot	عنوان مصدر الرسالة وعنوان مستقبلها
Source and destination IP address	برنامج في صورة المصدر
Source code	عنوان الحاسب المرسل
Source IP address	إرسال البريد الإلكتروني لآلاف المستفيدين
Spam mail	الشبكة الفرعية المحجوبة المقسمة
Split-screened subnet	التنصت
Spoofing	جدول الحالة
State table	مصفاة الحزم الاستاتيكية
Static packet filter	الشبكة الفرعية
Subnet	أنماط فرعية
Subpatterns	إقحام نسخة أخرى من البرنامج
Subversion	الحاسبات العملاقة
Super computers	المحولات

Symmetric cryptography	التشفير المتماثل
Synchronous Optical Network (SONET)	الشبكة الضوئية المتزامنة
System Administrator, Supervisor	مدير النظام
System logs	سجلات وقائع استخدام النظام
System shutdown	إنهاء النظام
System startup	تشغيل النظام
TCP flags	علامات حزم TCP
Teardrop attack	هجوم " قطرة الدمع "
Telemedicine	الطب عن بعد
Telnet service	خدمة الدخول عن بعد
Terrestrial microwave	أشعة الميكروويف الأرضية
Three?tier structure	بنية الطبقات الثلاث
Time of day	التوقيت
Time stamp	بصمة التوقيت
Timeout error	تجاوز الفترة الزمنية
Traffic log	سجل الوقائع للرسائل المارة بالشبكة
Trans-European Network	الشبكة الأوروبية
Transmission Control Protocol/ Internet Protocol (TCP/IP)	بروتوكول التحكم في النقل/ بروتوكول الإنترنت
Transponder	دائرة النقل
Triple DES	نظام التشفير الرقمي الثلاثي
Trivial FTP (TFTP)	خدمة نقل الملفات البسيطة
Trojan horse	حصان طروادة
Troubleshooting	البحث عن حل المشكلة

Trust	الثقة في المعلومات
Tunneling	أسلوب النفق في الاتصال
Twisted pair access to the information highway	وسيلة الوصول إلى طريق المعلومات السريع عن طريق خطوط الهاتف
two-way trust	الثقة المتبادلة
Two-wire open lines	الخطوط المزدوجة المفتوحة
Unauthorized access	الاستخدام غير المرخص به
United States Postal Service (USPS)	خدمة بريد الولايات المتحدة
Unshielded Twisted Pair (UTP)	الخطوط المزدوجة المجدولة غير المعزولة
Upper case	الحروف الكبيرة
User Datagram Protocol (UDP)	بروتوكول حزم المستخدم
User ID (UID)	رمز المستفيد
User Manager for Domains Utility	برنامج إدارة النطاقات
Utilities	البرامج المساعدة
Vampire worm	الدودة مصاصة الدماء
Very Small Aperture Terminals (VSAT)	محطات استقبال صغيرة
Virtual Private Network (VPN)	الشبكة الخاصة الافتراضية
Virtual reality	الواقع الافتراضي
Virtual universities	الجامعات الافتراضية
Virus	الفيروس
Virus scanners	فاحصات الفيروسات
VPN tunnel	نفق الشبكة الخاصة الافتراضية
Vulnerability assessment	تقييم درجة ضعف النظام
Web browsers	برامج استعراض الإنترنت

Web pages	صفحات الإنترنت
Web server	خادم الإنترنت
Web?based training	التدريب عن طريق الإنترنت
Wide Area Networks	الشبكات الكبيرة
Wireless Application Protocol (WAP)	بروتوكول التطبيقات اللاسلكية
Wireless ATM	النقل اللاسلكي غير المتزامن
World Wide Web	شبكة النسيج العالمية
Worm	دودة الحاسب
Worms Against Nuclear Killers (WANK)	الدودة النووية

الفهرس الموضوعي

C

D

P

R

S

المؤلف فى سطور

المهندس/ حسن أحمد طاهر داود

- من مواليد جمهورية مصر العربية في ١٩٤٦/٢/١٧م.

المؤهل العلمي:

- ماجستير هندسة الحاسب من جامعة جرينوبل بفرنسا يونيو ١٩٧٨م.
- بكالوريوس هندسة الاتصالات من جامعة عين شمس بالقاهرة يونيو ١٩٦٩م.

الوظيفة الحالية:

- عضو هيئة التدريس بقسم علوم الحاسب والمعلومات ومدير برنامج الحاسب الآلي - جامعة الأمير سلطان بالرياض.

الأنشطة العلمية:

- مجالات الاهتمام: أمن المعلومات، قواعد البيانات، شبكات المعلومات والإنترنت.
- مؤلف كتاب " جرائم نظم المعلومات " أكاديمية نايف العربية للعلوم الأمنية ٢٠٠٠م.
- مؤلف كتاب " الحاسب وأمن المعلومات " معهد الإدارة العامة ٢٠٠٠م.
- مؤلف كتاب " الأمن في عصر المعلومات " أكاديمية نايف العربية للعلوم الأمنية ٢٠٠٤م.

الأنشطة العملية:

- مدير تحرير المجلة العلمية المحكمة "**المعلوماتية والحوسبة التطبيقية**".
- أمين مجلس إدارة جمعية الحاسبات السعودية.
- عضو مجلس الأمانة العامة للخطة الوطنية **لتقنية المعلومات بالمملكة العربية السعودية**.
- منح عام ١٩٩٦ الجائزة العالمية: (The World Lifetime Achievement Award) من مؤسسة (American Biographical Institute) الأمريكية **تقديراً لجهوده في** خدمة مجتمع الحاسب **الآلي** بالمملكة.
- تم اختياره في عام ١٩٩٨م من قبل مؤسسة: (International Biographical Center) ومقرها بريطانيا ضمن المتميزين إبداعياً خلال القرن عن نشاطاته في مجال الحاسب الآلي.



تم التصميم والإخراج الفنى والطباعة فى
الإدارة العامة للطباعة والنشر بمعهد الإدارة العامة -١٤٢٥هـ

هذا الكتاب

المعلومات هي سمة العصر الذي نعيشه، وشبكات المعلومات هي الخلايا العصبية التي تتولى نقل المعلومات إلى كل مكان .. ومثلما حملت المعلومات، عبر رحلتها خلال الشبكات، آفاقًا جديدة للبشرية، فإنها حملت قدرًا مماثلاً من المخاوف الأمنية، خاصة مع طوفان الإنترنت الذي كاد يغرق الجميع. وزادت المخاطر التي تهدد المعلومات، وفي الوقت نفسه ظهرت أجهزة وتقنيات تقاوم كل أساليب انتهاك المعلومات .. بل وتجهضها قبل أن تولد .. وكان لابد من الإحاطة بكل ذلك .. بالخطر القائم وبوسائل مواجهته؛ فجاء هذا الكتاب ليسد النقص الكبير في المكتبة العربية بتغطيته لموضوع " أمن شبكات المعلومات ".

يتناول الكتاب الأمن في عصر المعلومات، ثم يقدم الخلفية التقنية الضرورية للقارئ عن أساليب نقل المعلومات عبر الشبكات، وبروتوكولات نقل البيانات، والتقنيات الحديثة المستخدمة في شبكات المعلومات ومستقبلها.

ثم يتطرق للسياسة الأمنية للمؤسسات، ثم يستعرض أساليب انتهاك شبكات المعلومات بمختلف أنواعها مع سيناريو كامل لعمليات الاقتحام وخطواتها، ولا يغفل الحديث عن الفيروسات وعن التشفير، ومتطلبات البنية الأساسية للمفتاح العلني، والتوقيعات الرقمية.

يتناول الكتاب كذلك نظم كشف الاقتحام وتقييمها ، ويشرح عمل جدران الحماية وخوادم البروكسي، ثم يتناول تقنية الشبكات الخاصة الافتراضية واستخداماتها ومزاياها وعيوبها.

يتناول الكتاب كذلك كيفية ملاحقة المهاجمين لشبكات المعلومات، وينتهي بتقييم مستوى الأمن في نظم تشغيل الشبكات الشهيرة (نتوير وويندوز إن تي ويونكس).

وينتهي الكتاب بمسردين للمصطلحات الفنية والترجمة المقابلة لها (باللغتين العربية والإنجليزية).

ردمك : ٩٩٦٠-١٤-١٠٨-X-

تصميم وإخراج وطباعة الإدارة العامة للطباعة والنشر - معهد الإدارة العامة ١٤٢٥هـ